５３．相互に暗号データの転送を実行する第１の装置と第２の装置とからなるデータ処理システムにおけるデータ処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、

上記第１の装置から上記第２の装置に転送されるコマンド識別子を予め定められた設定シーケンスにしたがって受領し、該受領コマンド識別子に対応するコマンドをレジスタから取り出して実行させるコマンド処理制御ステップを有し、

上記コマンド処理制御ステップにおいて、上記第１の装置から転送されるコマンド識別子が上記設定シーケンスと異なるコマンド識別子である場合には、該コマンド識別子に対応するコマンドの処理を中止するステップを含むことを特徴とするプログラム提供媒体。

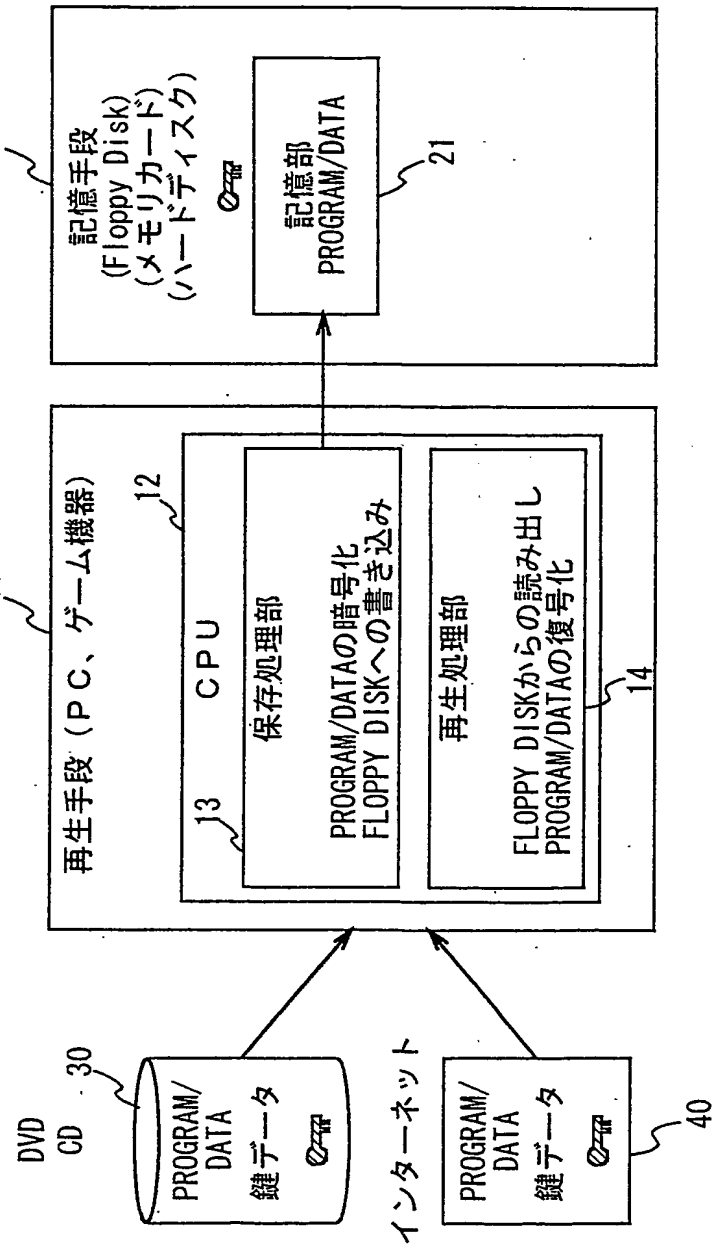

20
記憶手段
(Floppy Disk)
(メモリカード)
(ハードディスク)
記憶部
PROGRAM/DATA
21
10
再生手段（ＰＣ、ゲーム機器）
12
ＣＰＵ
13
保存処理部
PROGRAM/DATAの暗号化
FLOPPY DISKへの書き込み
再生処理部
FLOPPY DISKからの読み出し
PROGRAM/DATAの復号化
14
DVD
CD
30
PROGRAM/
DATA
鍵データ
インターネット
PROGRAM/
DATA
鍵データ
40

図１

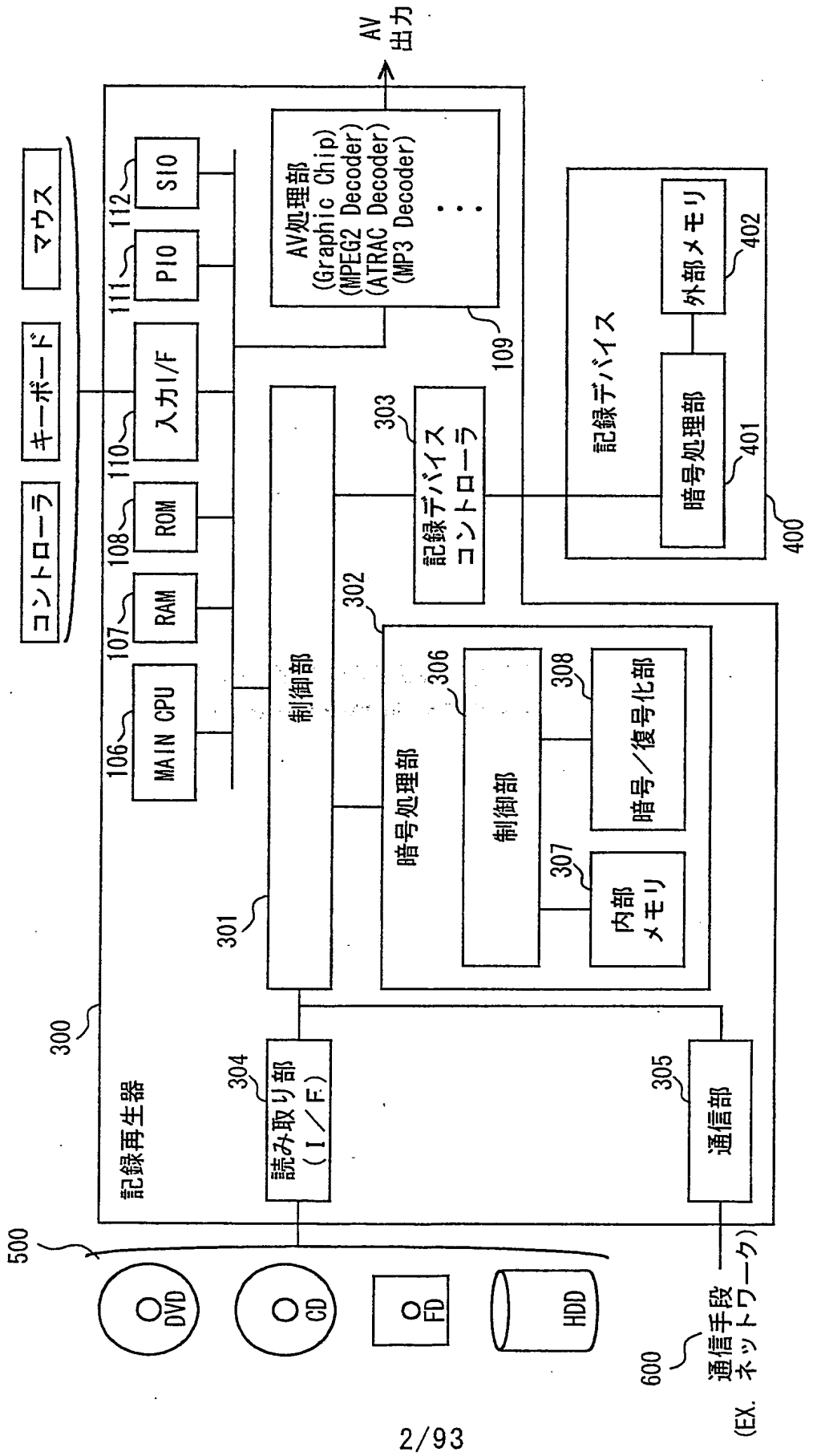

AV
出力
マウス
キーボード
コントローラ
SIO
PIO
入力I/F
ROM
RAM
MAIN CPU
AV処理部
(Graphic Chip)
(MPEG2 Decoder)
(ATRAC Decoder)
(MP3 Decoder)
109
111
112
110
108
107
106
303
記録デバイス
コントローラ
制御部
302
301
暗号処理部
306
制御部
308
暗号／復号化部
307
内部
メモリ
記録デバイス
外部メモリ
402
暗号処理部
401
400
300
記録再生器
304
読み取り部
(I／F.)
305
通信部
500
DVD
CD
FD
HDD
600
通信手段
ネットワーク
(EX.

図2

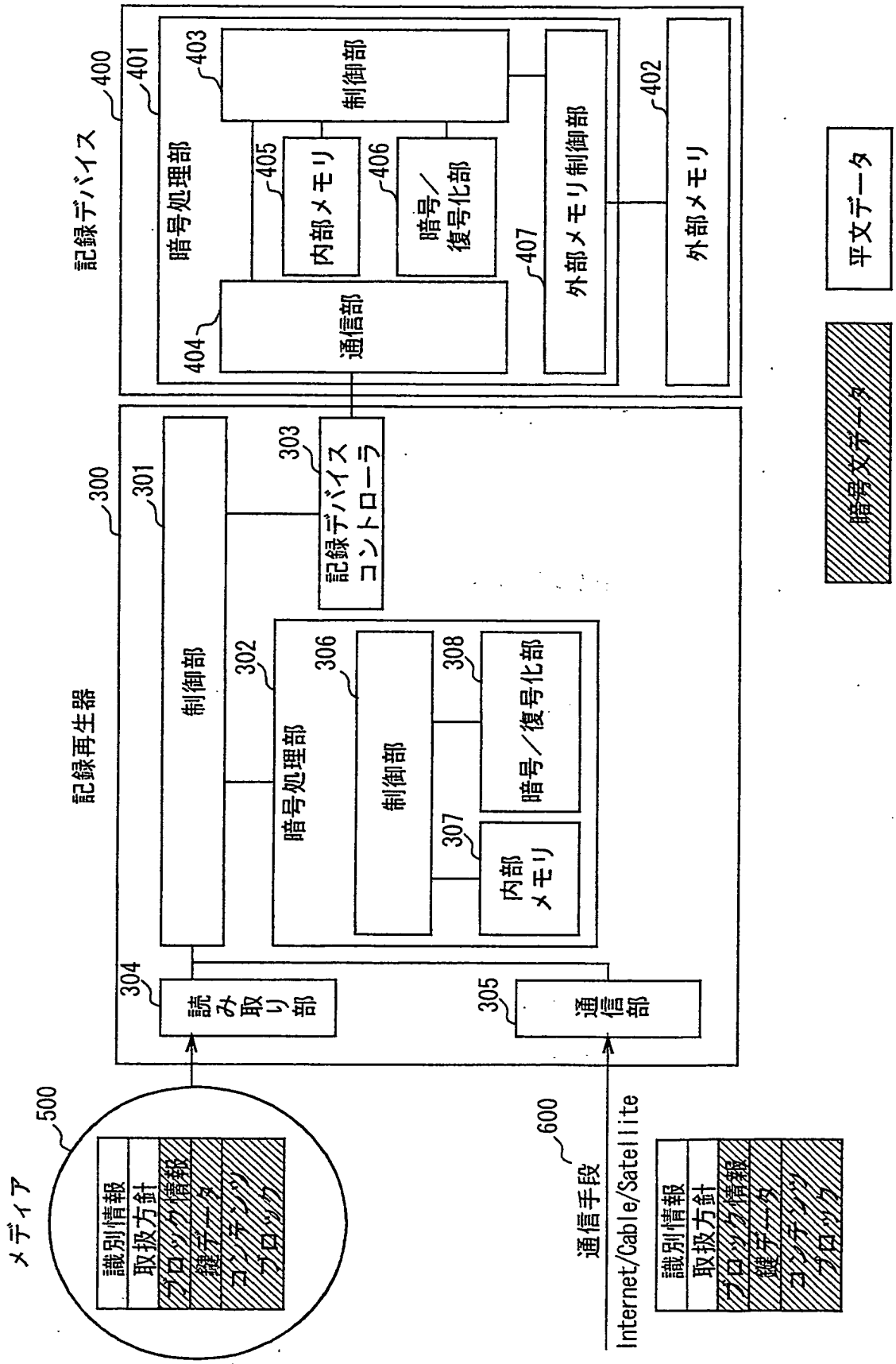

メディア
500
識別情報
取扱方針
プログラム情報
鍵データ
コンテンツ
プログラム
記録再生器
300
301
制御部
303
記録デバイス
コントローラ
302
暗号処理部
306
制御部
308
暗号／復号化部
307
内部
メモリ
304
読み
取り
部
305
通信部
記録デバイス
400
401
暗号処理部
403
制御部
405
内部メモリ
406
暗号／
復号化部
404
通信部
407
外部メモリ制御部
402
外部メモリ
600
通信手段
Internet/Cable/Satellite
識別情報
取扱方針
プログラム情報
鍵データ
コンテンツ
プログラム
暗号文データ
平文データ

図3

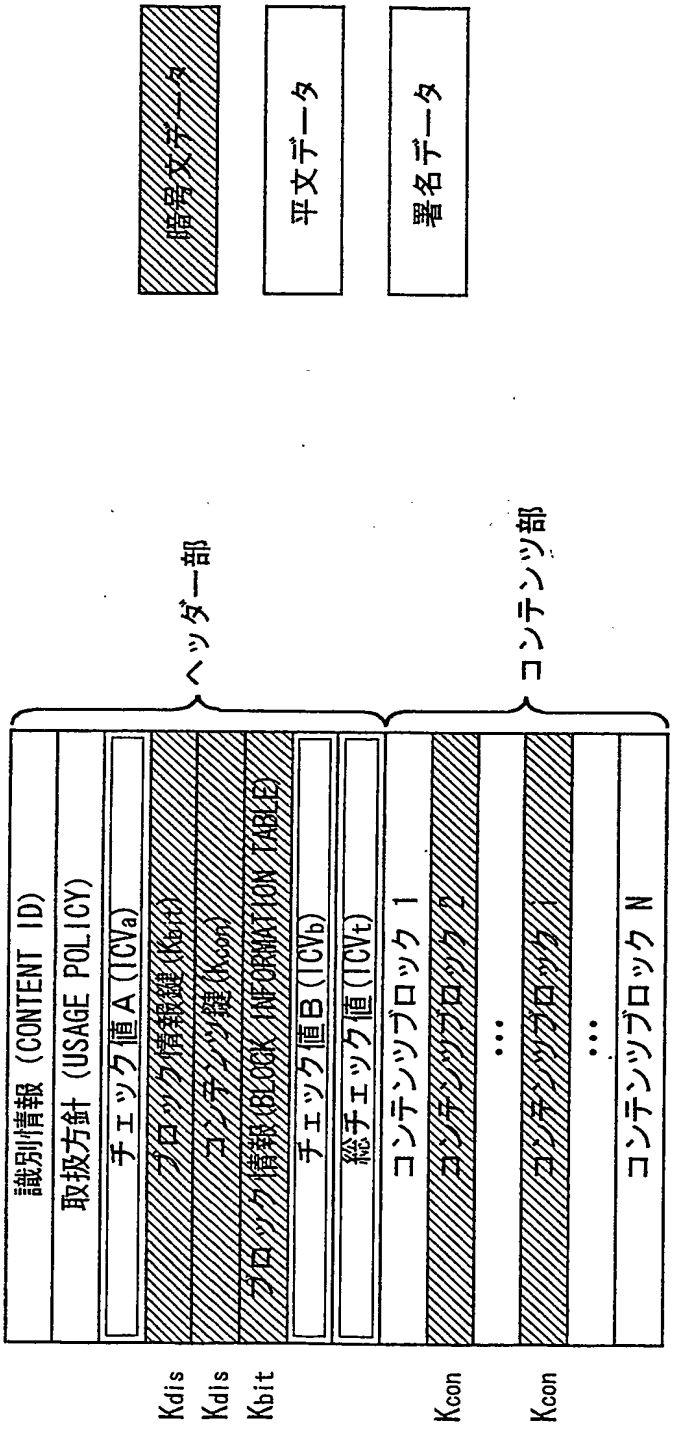


図4

メディア上及び通信路上のデータフォーマット

ヘッダーサイズ (Header Length)
コンテンツサイズ (Content Length)
フォーマットバージョン (Format Version)
フォーマットタイプ (Format Type)
コンテンツタイプ (Content Type)
起動優先順位情報 (Operation Priority)
利用制限情報 (Localization Field)
複製制限情報 (Copy Permission)
移動制限情報 (Move Permission)
暗号アルゴリズム (Encryption Algorithm)
暗号化モード (Encryption Mode)
検証方法 (Integrity Check Method)

取扱方針

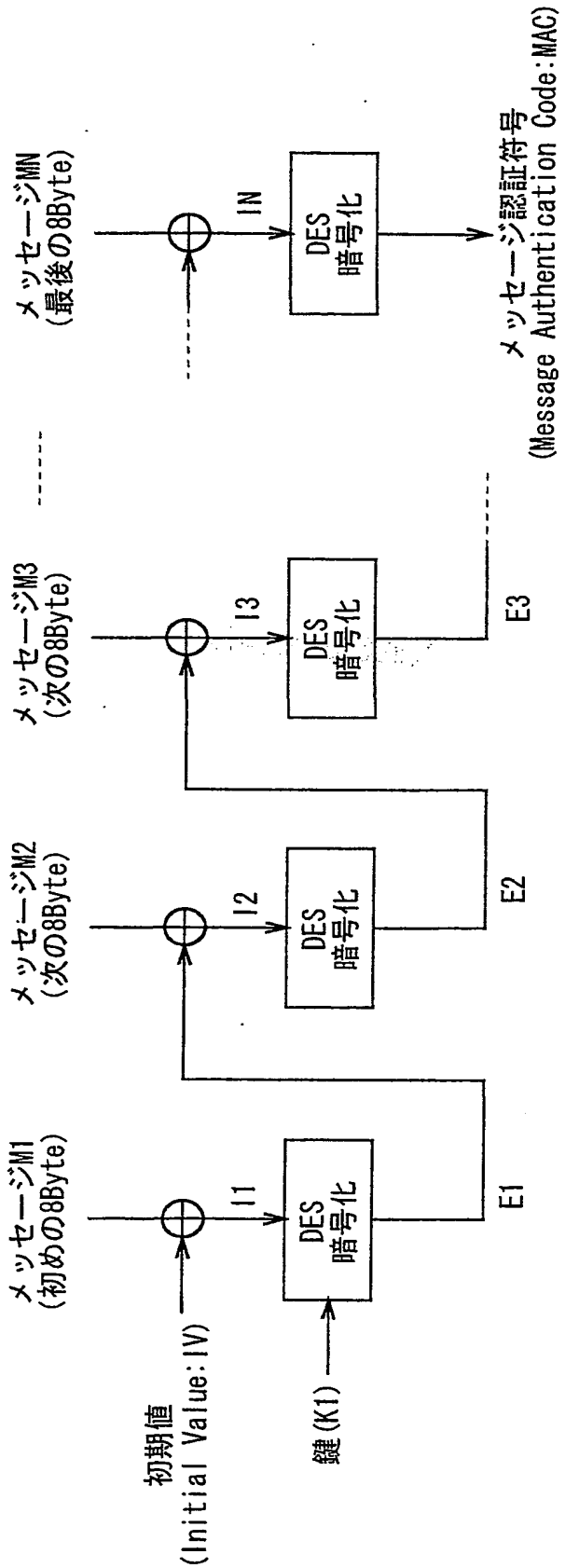
図５

Kbit

	コンテンツブロック数（Block Number）
ブロック1	ブロックサイズ（Block Length）
	暗号化フラグ（Encryption Flag）
	検証対象フラグ（ICV Flag）
	コンテンツチェック値（ICV1）
	・ ・ ・ ・
ブロックN	ブロックサイズ（Block Length）
	暗号化フラグ（Encryption Flag）
	検証対象フラグ（ICV Flag）
	コンテンツチェック値（ICVN）

ブロック情報

図６



⊕:排他的論理和処理 (8バイト単位)

図7

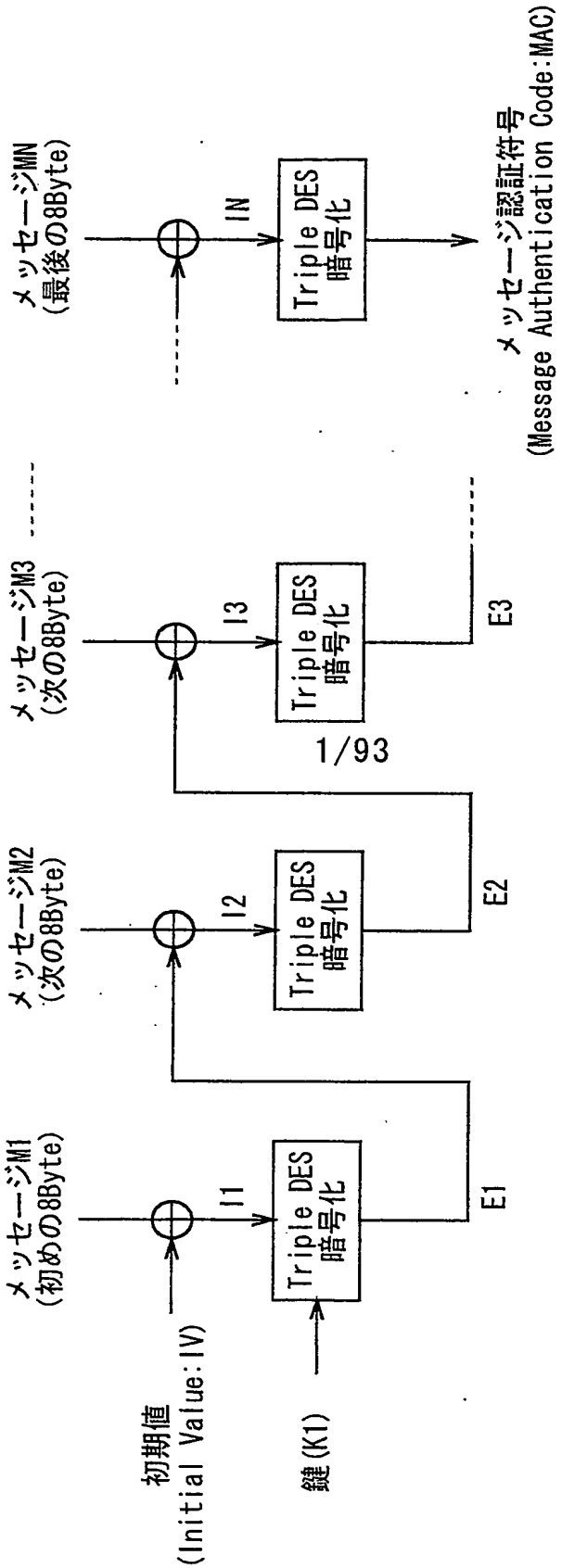
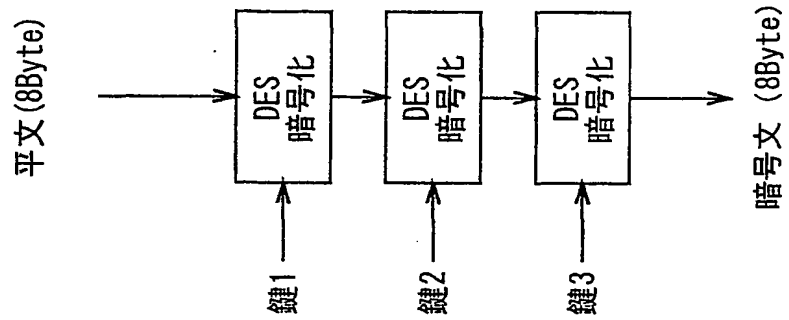

メッセージM1
(初めの8Byte)
メッセージM2
(次の8Byte)
メッセージM3
(次の8Byte)
メッセージMN
(最後の8Byte)
初期値
(Initial Value:IV)
鍵(K1)
I1
I2
I3
IN
Triple DES
暗号化
E1
E2
E3
メッセージ認証符号
(Message Authentication Code:MAC)

図8


平文(8Byte)
DES 暗号化
DES 暗号化
DES 暗号化
暗号文 (8Byte)
鍵1
鍵2
鍵3
(b)

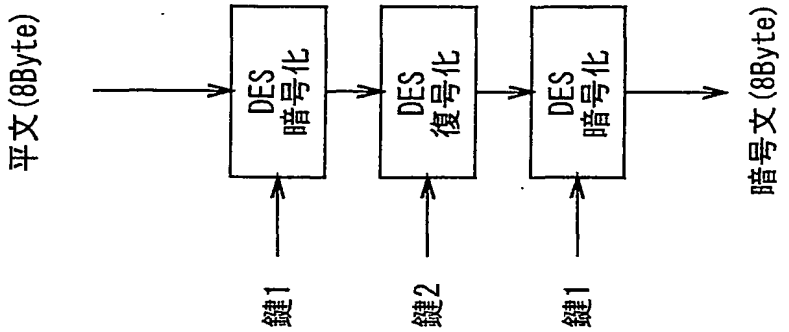

平文(8Byte)
DES 暗号化
DES 復号化
DES 暗号化
暗号文(8Byte)
鍵1
鍵2
鍵1
(a)

図9

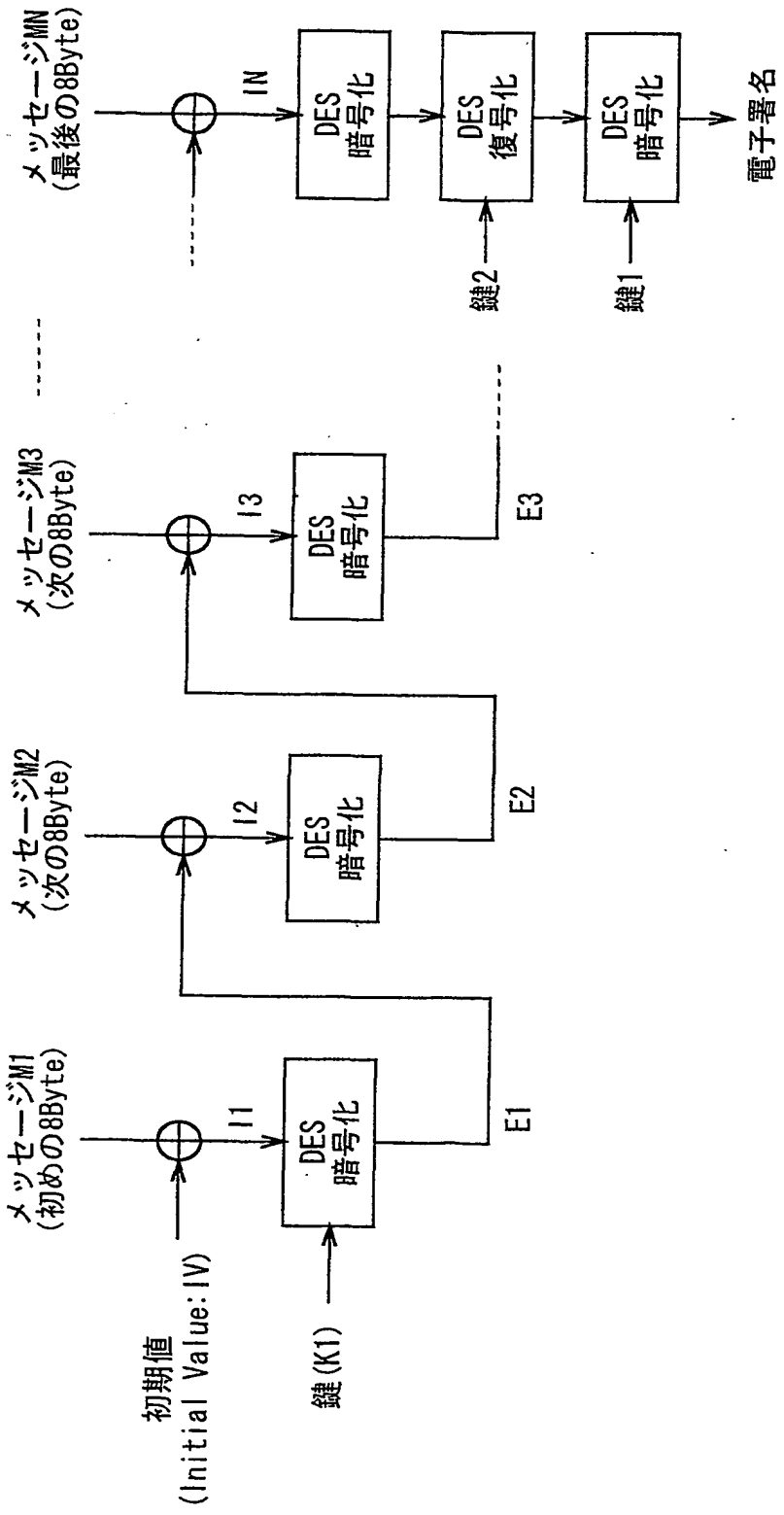
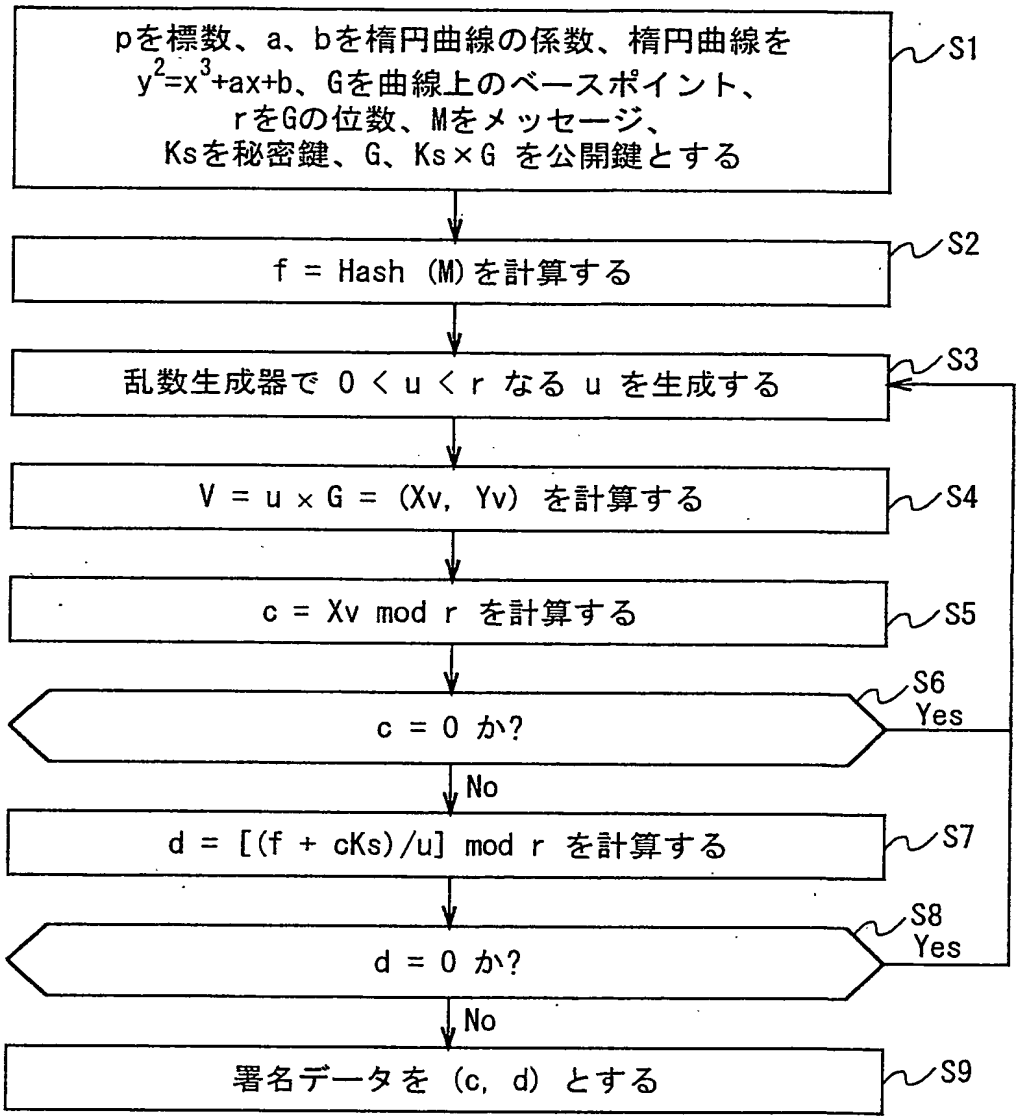

メッセージM1
(初めの8Byte)
メッセージM2
(次の8Byte)
メッセージM3
(次の8Byte)
メッセージMN
(最後の8Byte)
初期値
(Initial Value:IV)
鍵(K1)
I1
I2
I3
IN
DES
暗号化
DES
復号化
DES
暗号化
E1
E2
E3
鍵2
鍵1
電子署名

図１０

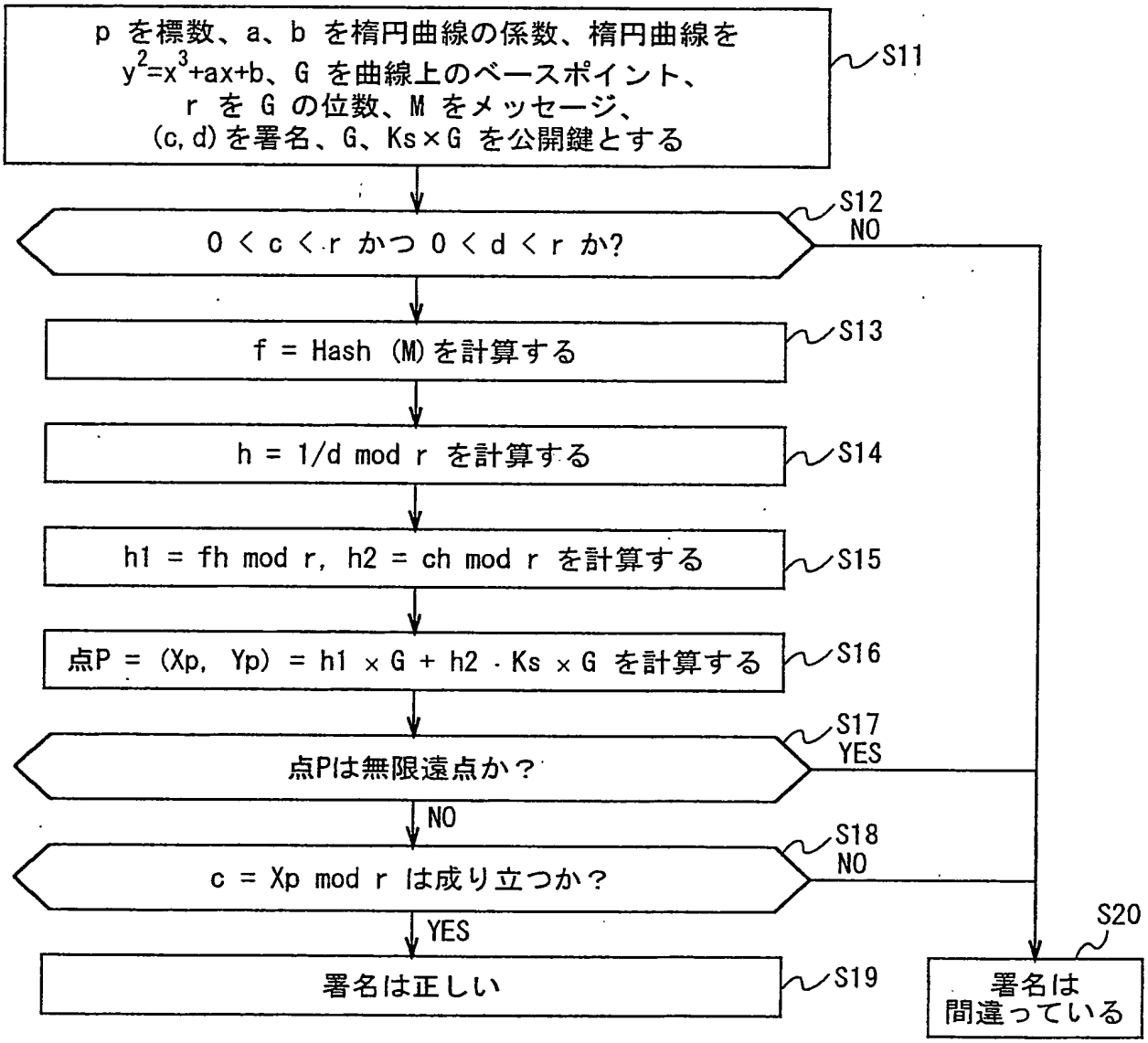
署名生成



署名生成 (IEEE P1363/D3)

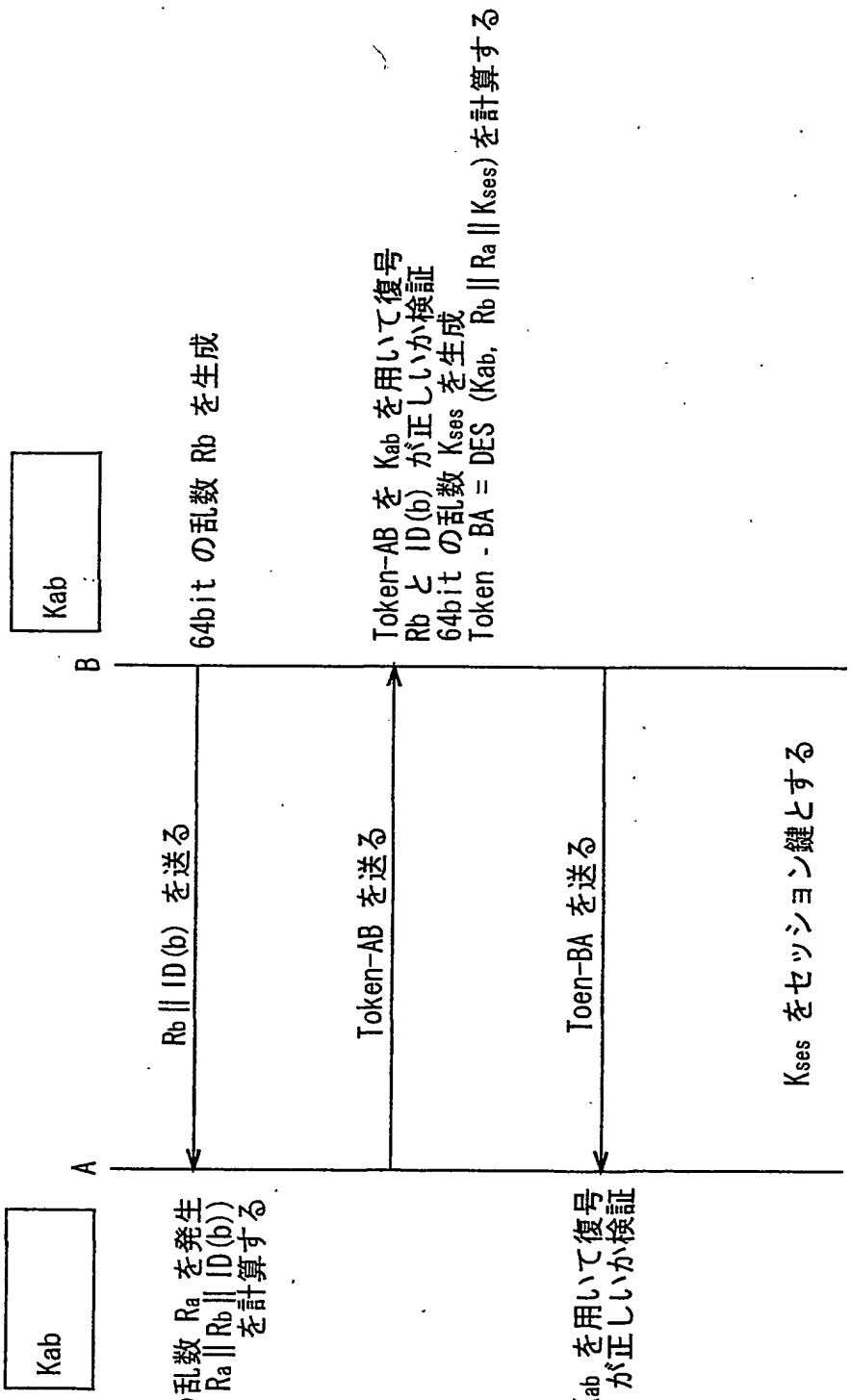
図１１

署名検証



署名検証(IEEE P1363/D3)

図１２



ISO/IEC 9798-2 対称鍵暗号鍵技術を用いた相互認証および鍵共有方式

図13

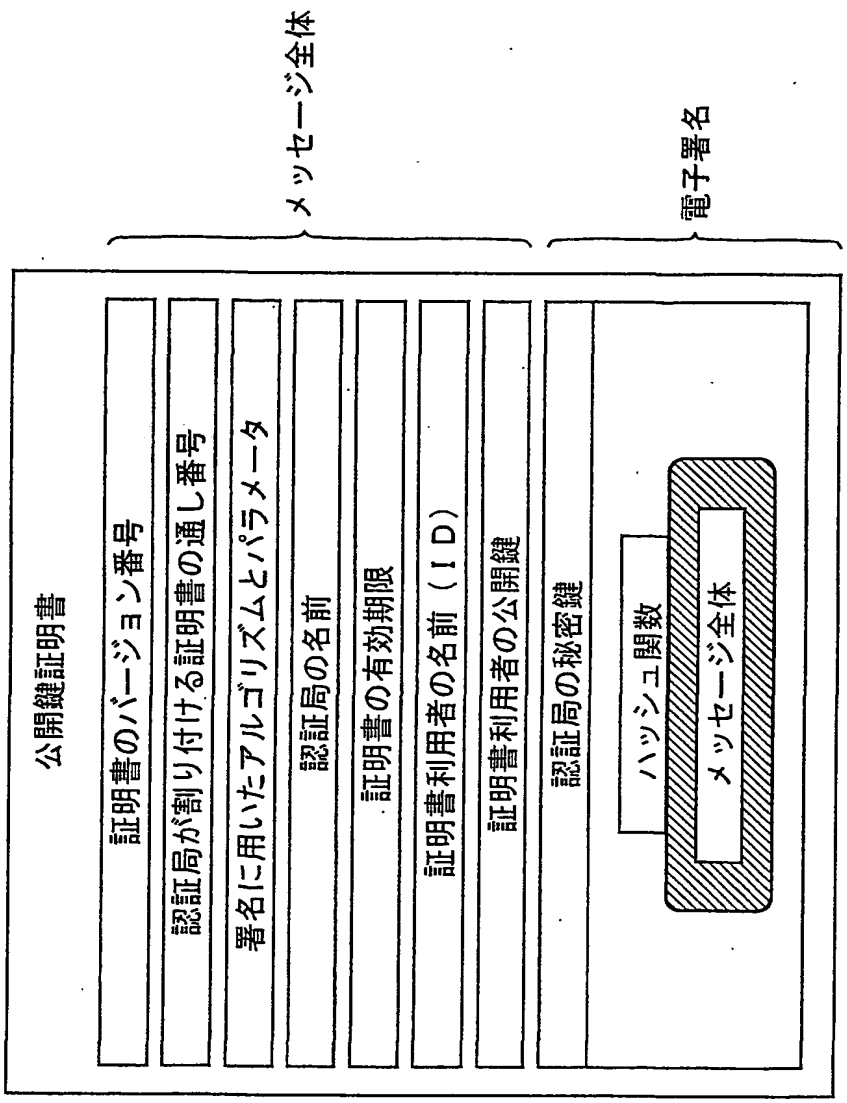
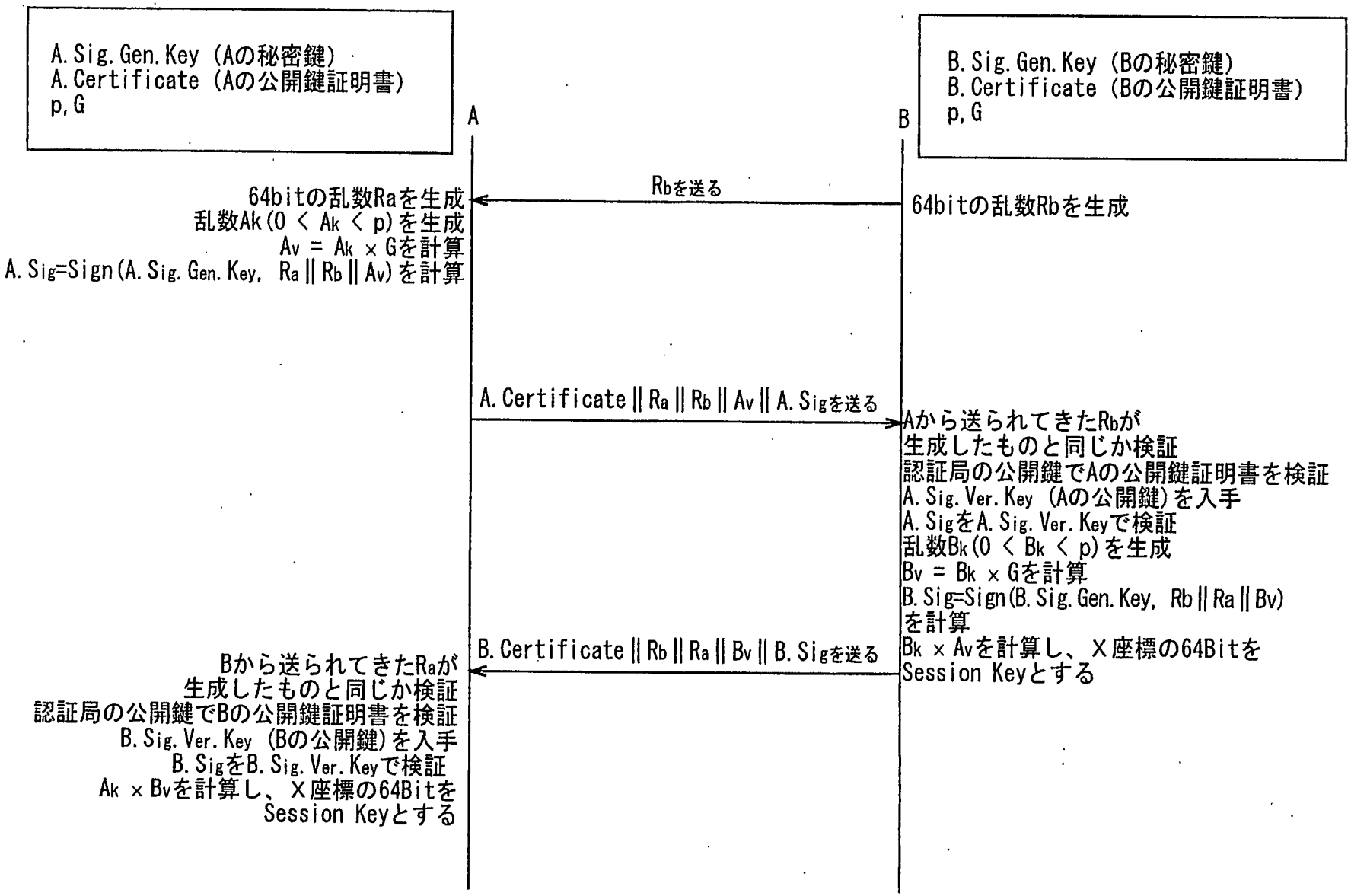

公開鍵証明書
証明書のバージョン番号
認証局が割り付ける証明書の通し番号
署名に用いたアルゴリズムとパラメータ
認証局の名前
証明書の有効期限
証明書利用者の名前（ＩＤ）
証明書利用者の公開鍵
認証局の秘密鍵
ハッシュ関数
メッセージ全体
メッセージ全体
電子署名
公開鍵証明書

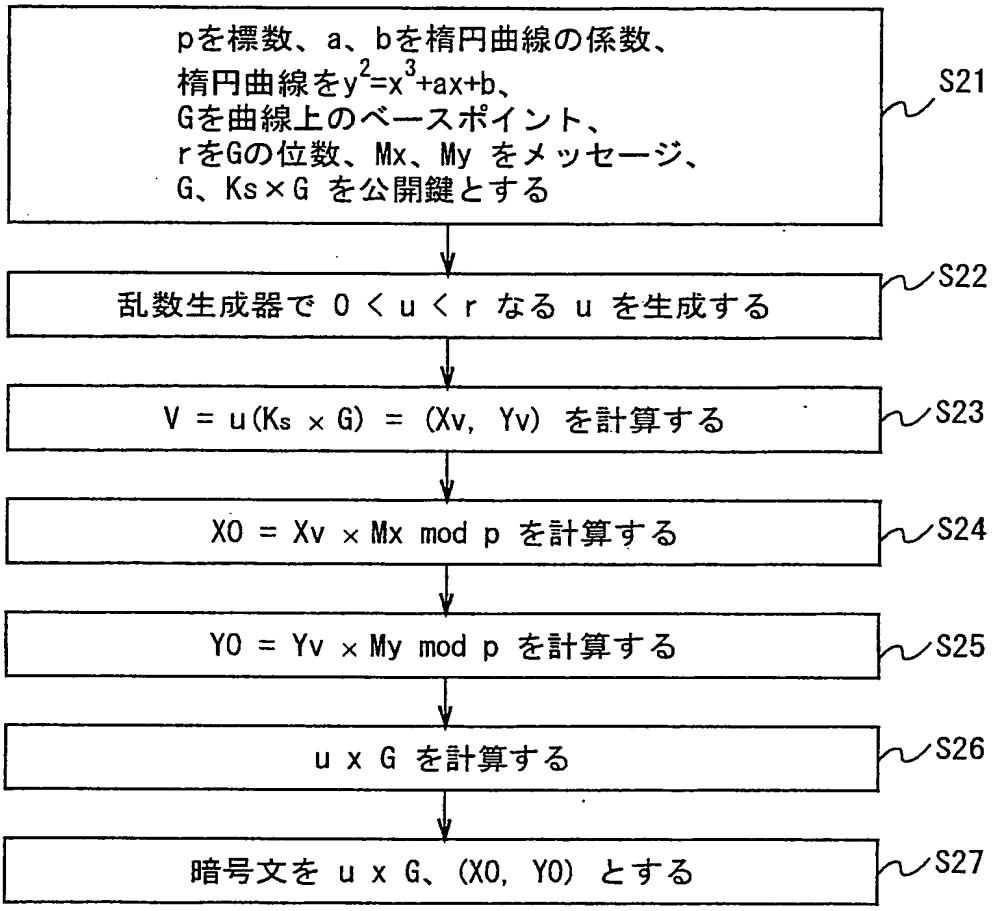
図１４



ISO/IEC 9798-3 非対称鍵暗号技術を用いた相互認証および鍵共有方式

図１５

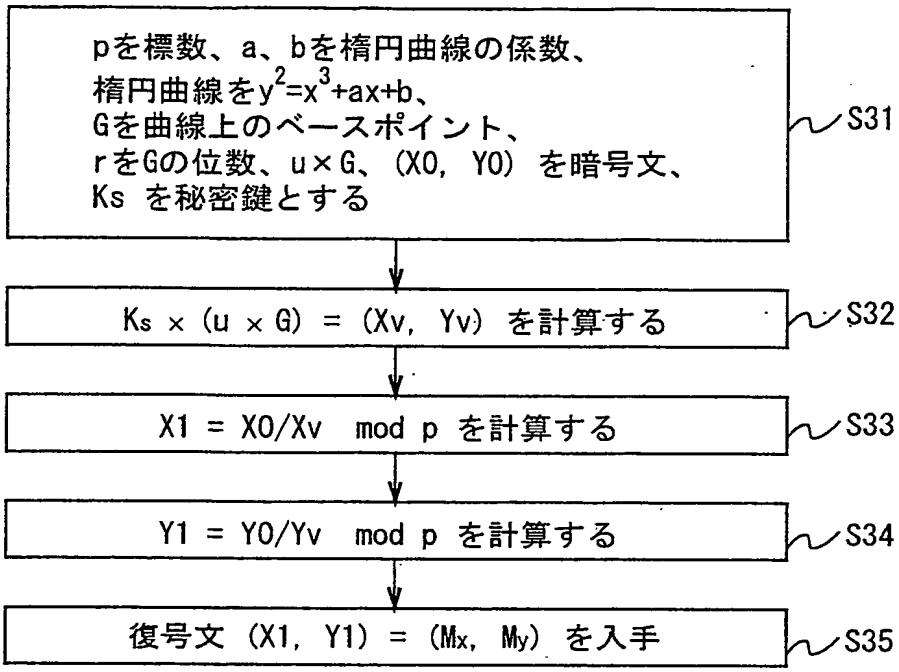
暗号化



楕円曲線暗号を用いた暗号化(Menezens-Vanstone)

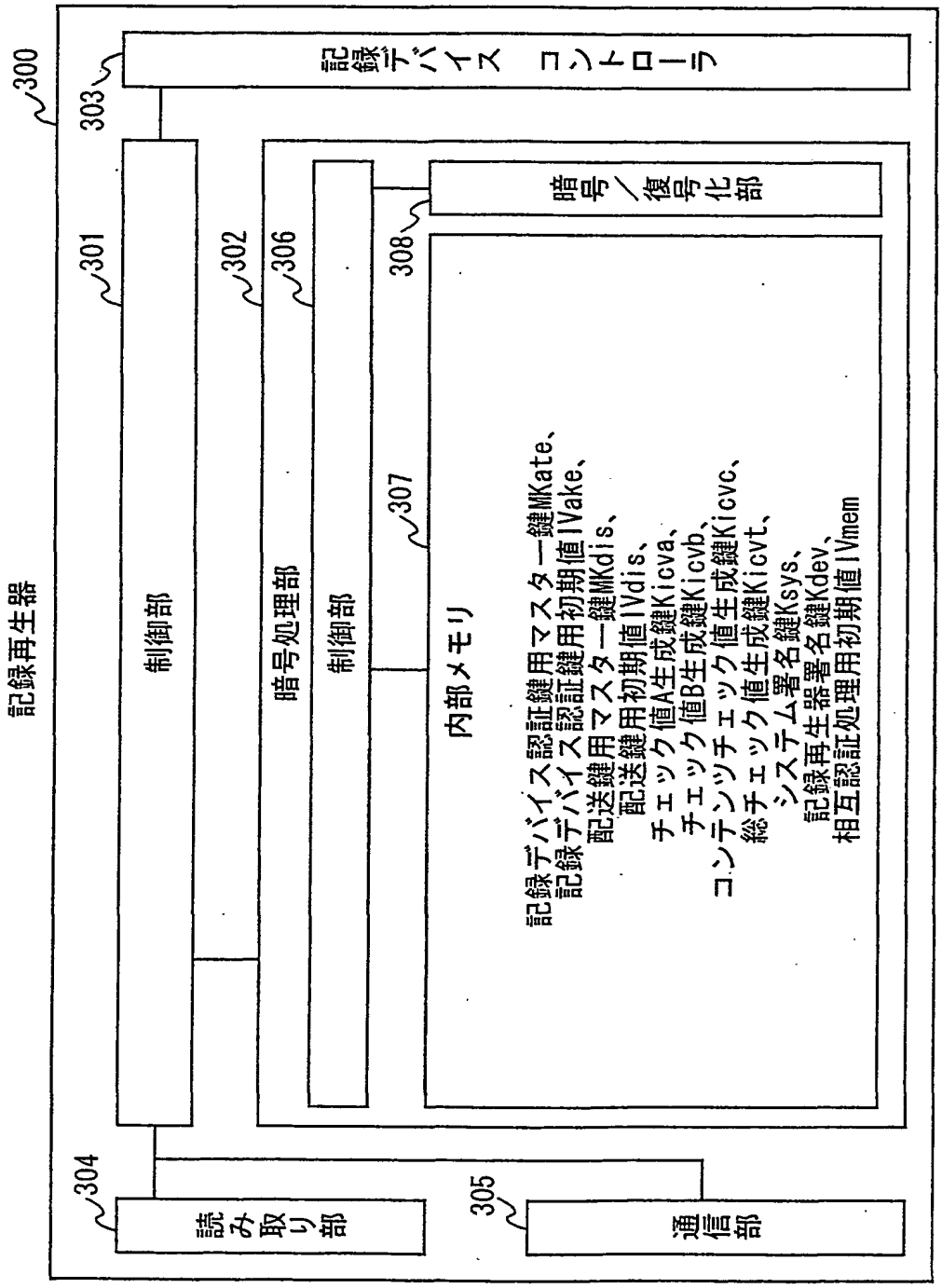
図１６

復号化



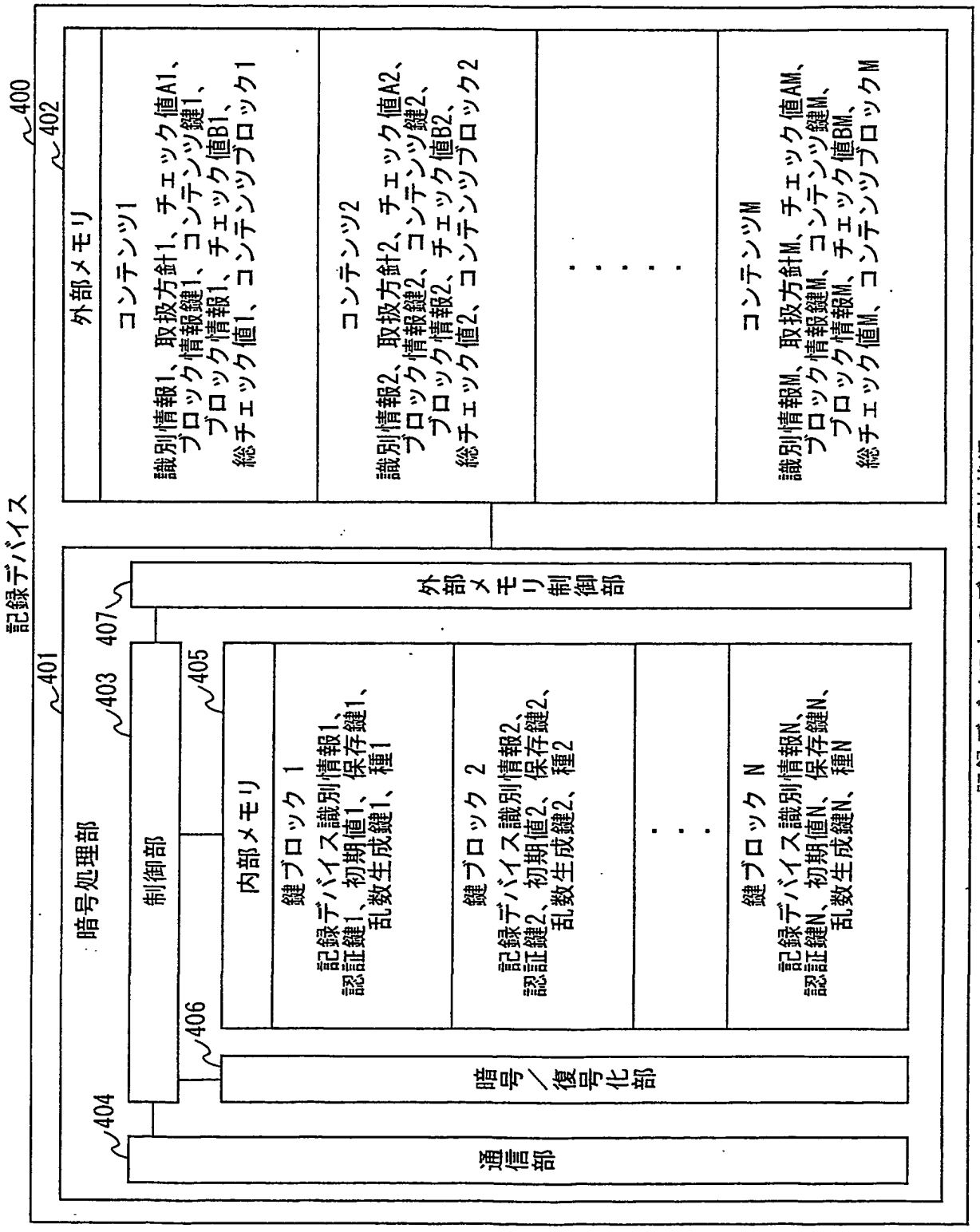
楕円曲線暗号を用いた復号化(Menezes-Vanstone)

図１７



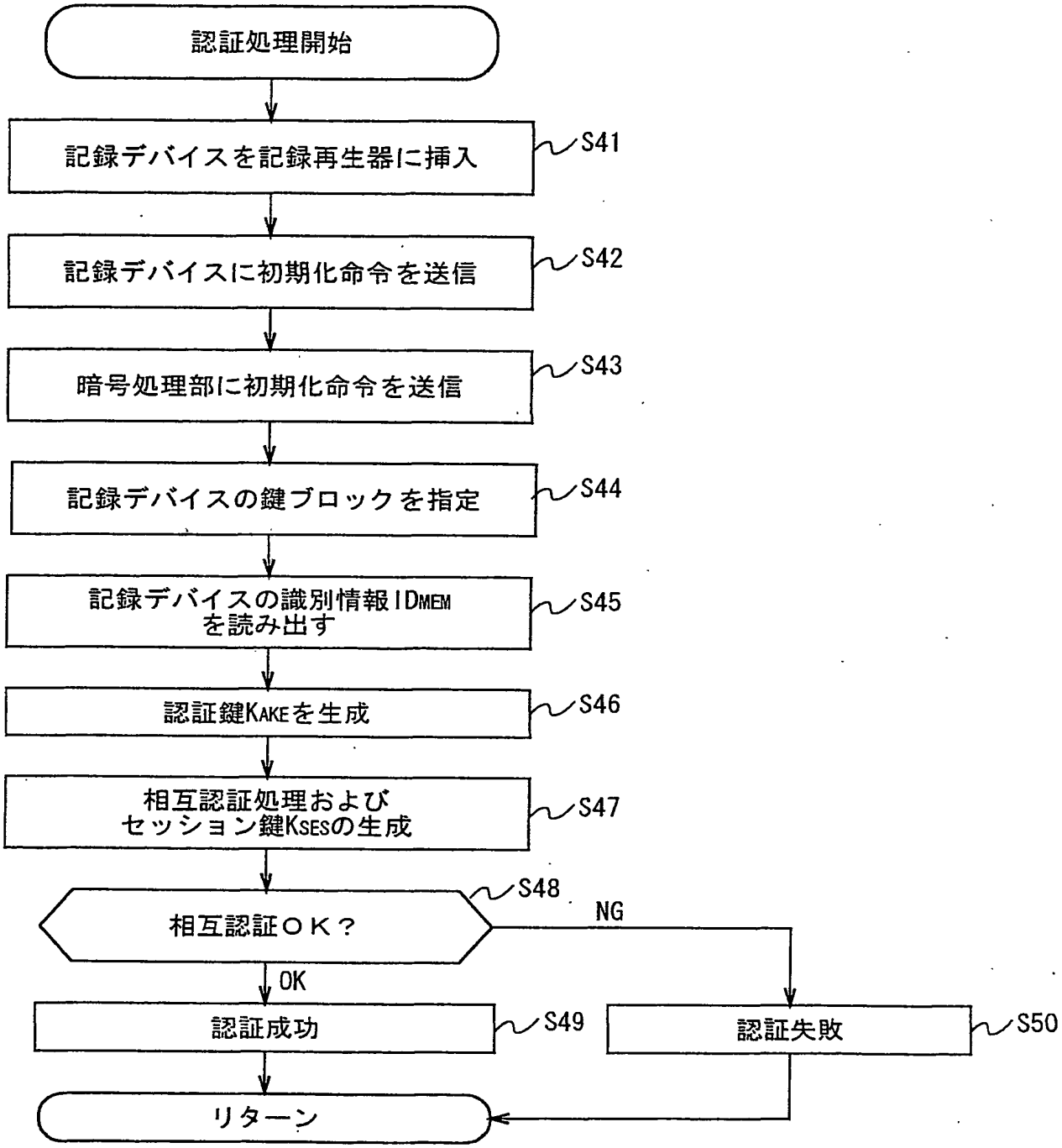
記録再生器上のデータ保持状況

図１８



記録デバイス上のデータ保持状況

図１９



記録再生器と記録デバイスとの相互認証

図２０

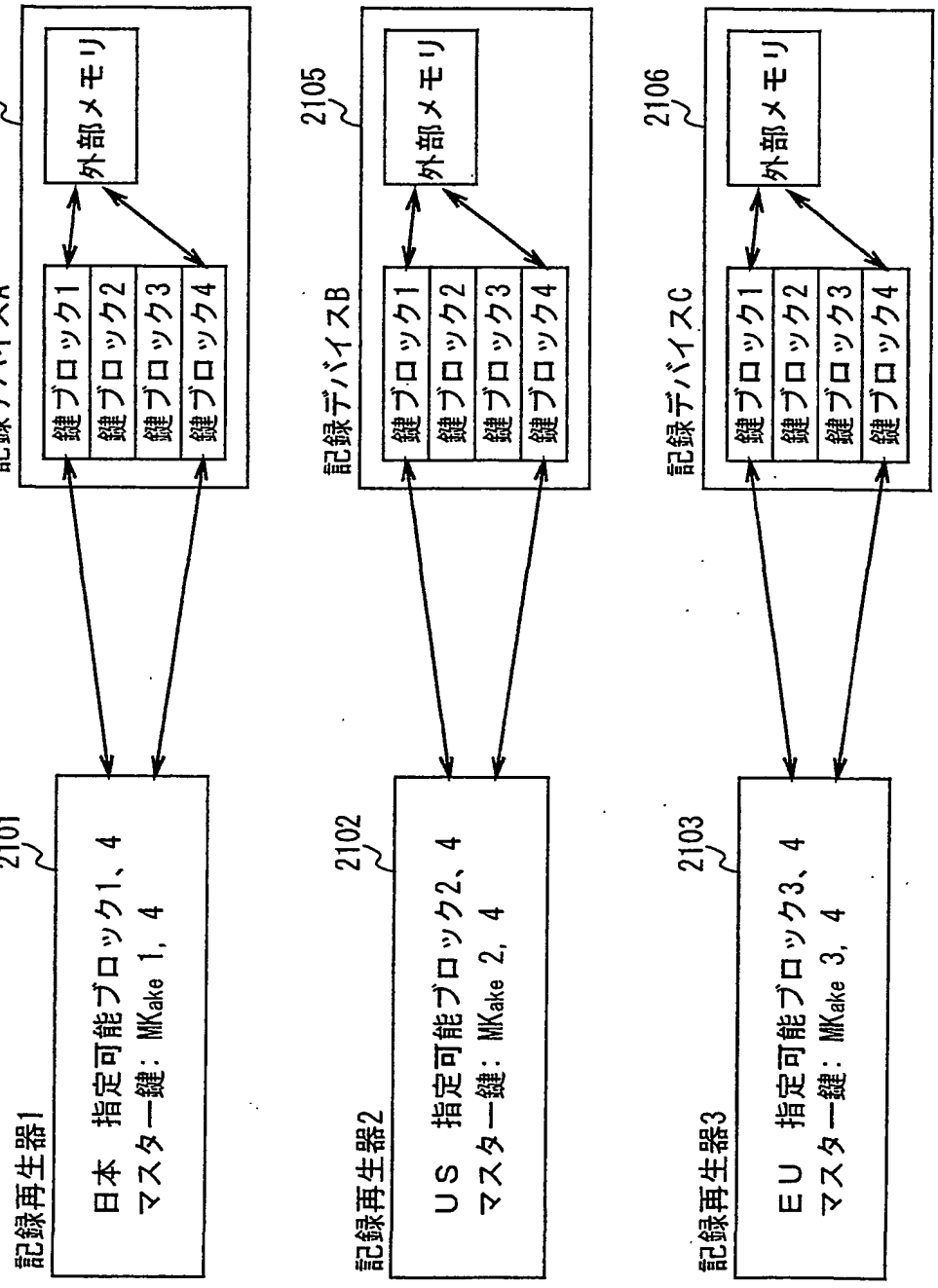
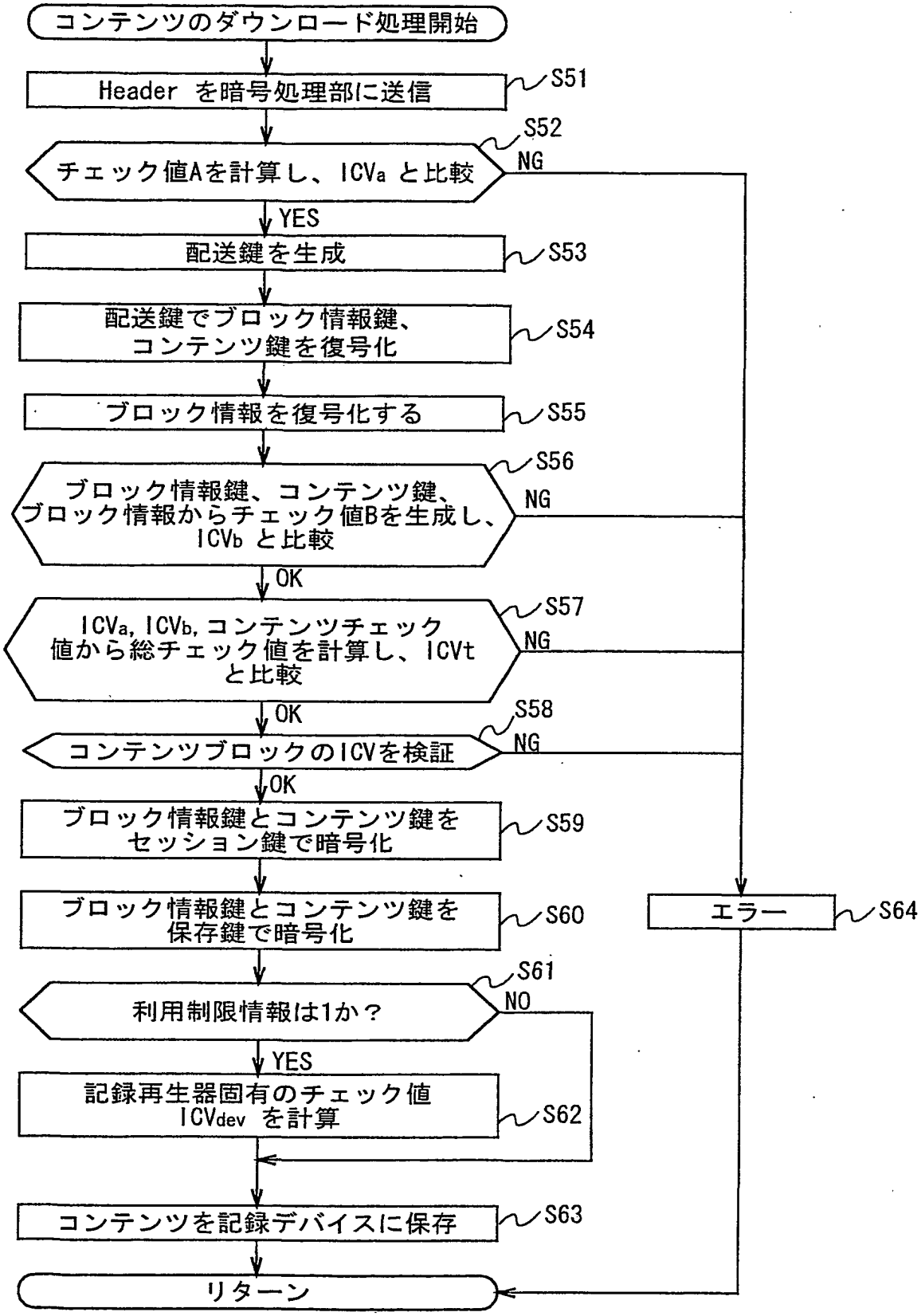
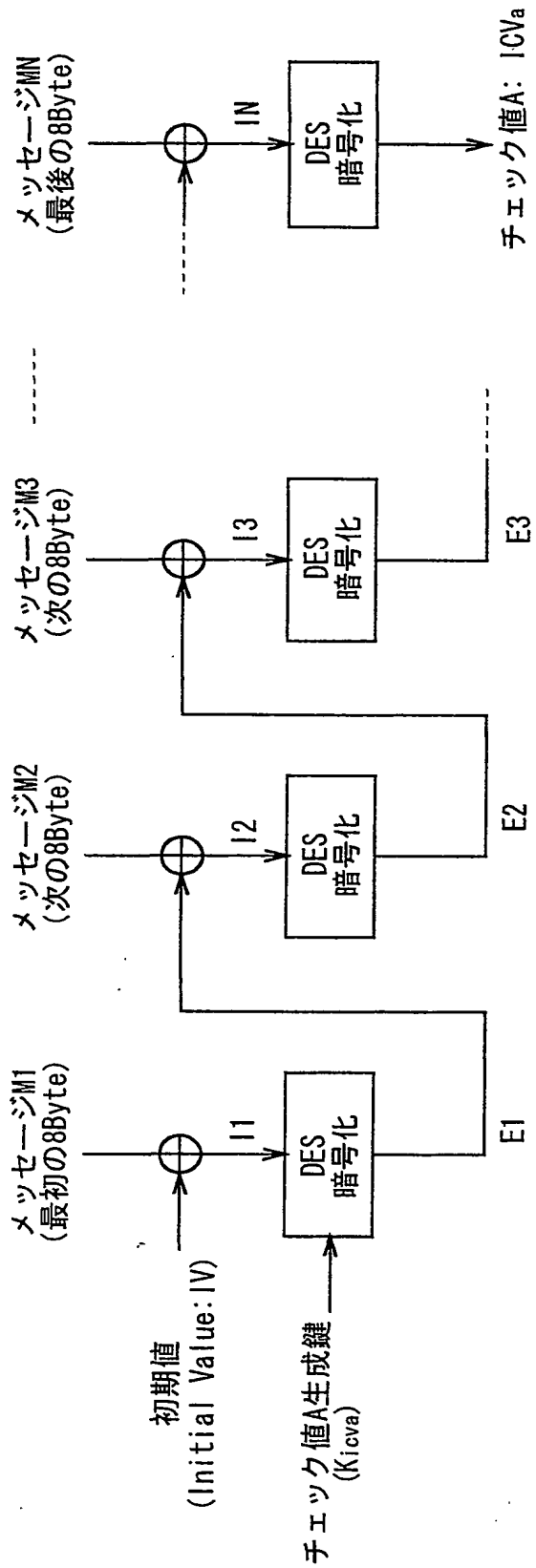

2104
外部メモリ
記録デバイスA
鍵ブロック1
鍵ブロック2
鍵ブロック3
鍵ブロック4
2101
記録再生器1
日本 指定可能ブロック1、4
マスター鍵：MKake 1, 4
2105
外部メモリ
記録デバイスB
鍵ブロック1
鍵ブロック2
鍵ブロック3
鍵ブロック4
2102
記録再生器2
ＵＳ 指定可能ブロック2、4
マスター鍵：MKake 2, 4
2106
外部メモリ
記録デバイスC
鍵ブロック1
鍵ブロック2
鍵ブロック3
鍵ブロック4
2103
記録再生器3
ＥＵ 指定可能ブロック3、4
マスター鍵：MKake 3, 4

図２１



コンテンツのダウンロード処理

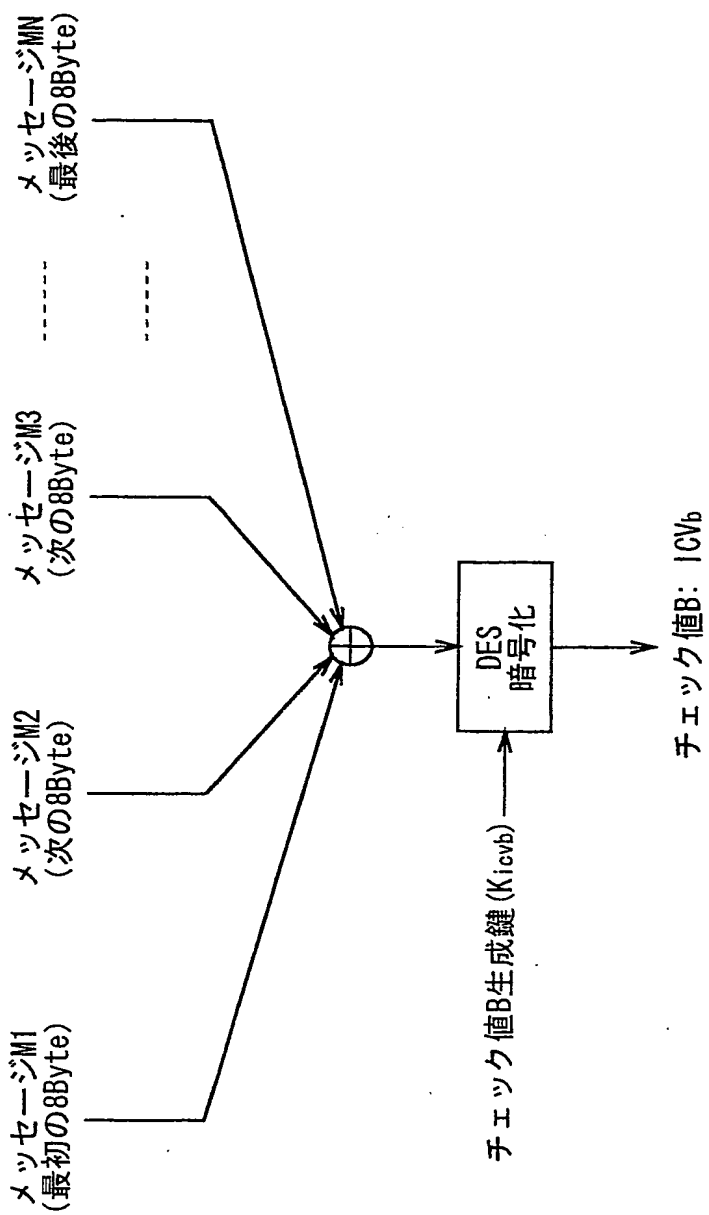
図２２



メッセージM1～MN:識別情報、取扱方針

⊕:排他的論理和処理 (8バイト単位)

図23



メッセージM1～MN : ブロック情報鍵 Kbit, コンテンツ鍵 Kcon, ブロック情報
⊕:排他的論理和処理 (8バイト単位)

図２４

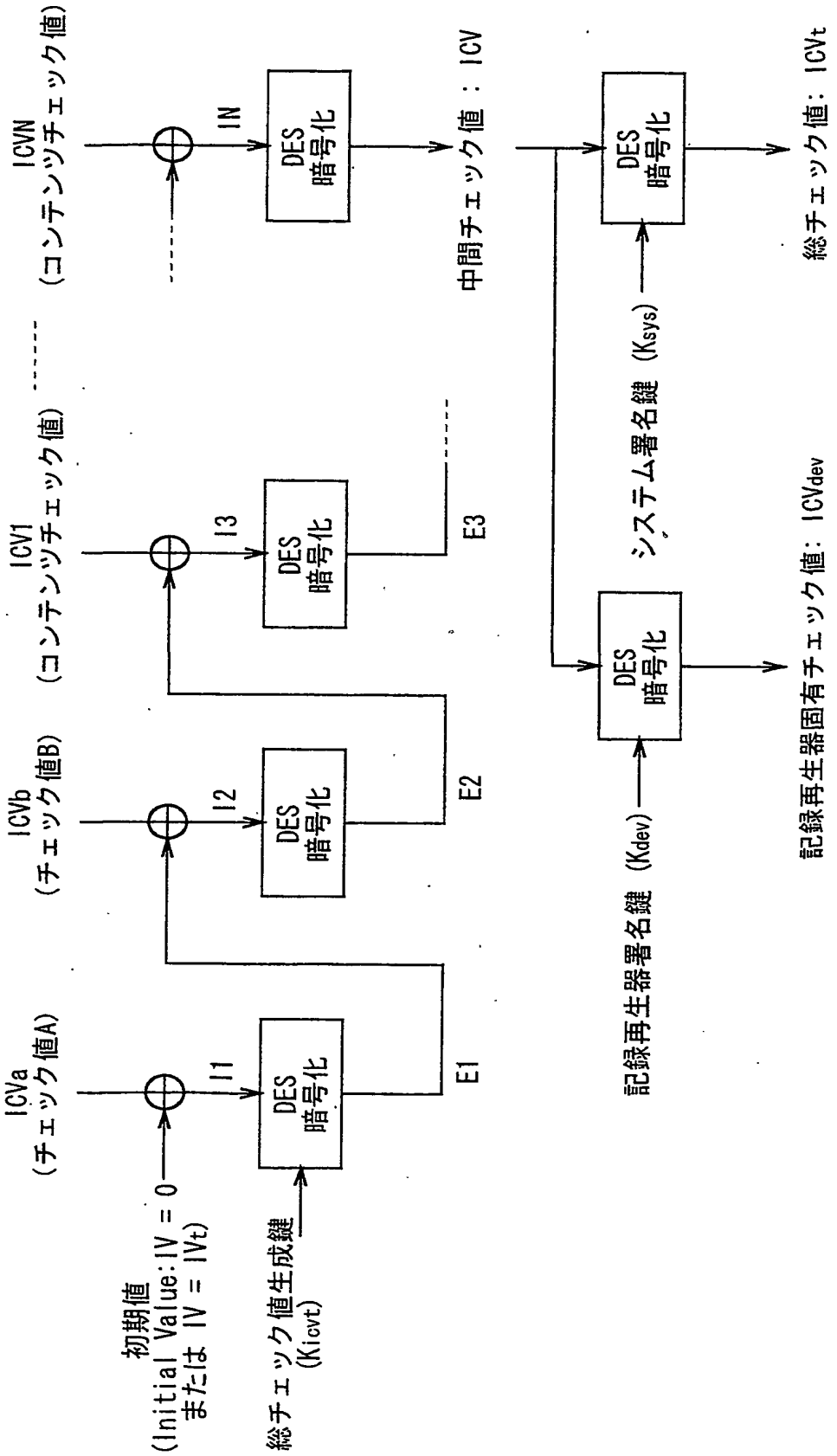

初期値
(Initial Value:IV = 0
または IV = IVt)
総チェック値生成鍵
(Kicvt)
ICVa
(チェック値A)
ICVb
(チェック値B)
ICV1
(コンテンツチェック値)
ICVN
(コンテンツチェック値)
I1
I2
I3
IN
DES
暗号化
E1
E2
E3
中間チェック値 : ICV
記録再生器署名鍵 (Kdev)
システム署名鍵 (Ksys)
記録再生器固有チェック値: ICVdev
総チェック値: ICVt
⊕:排他的論理和処理 (8バイト単位)

図２５

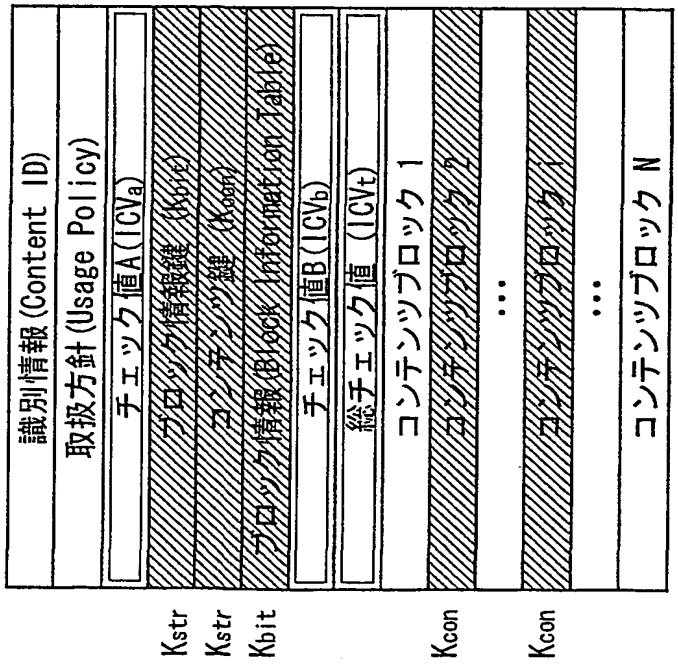
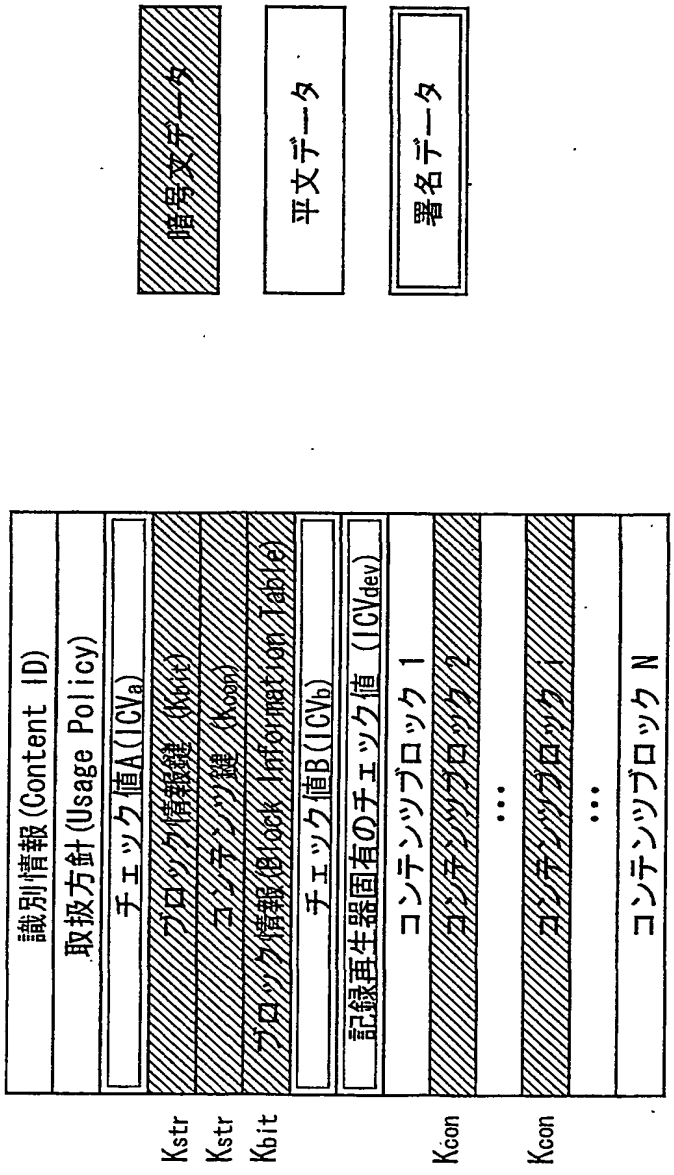
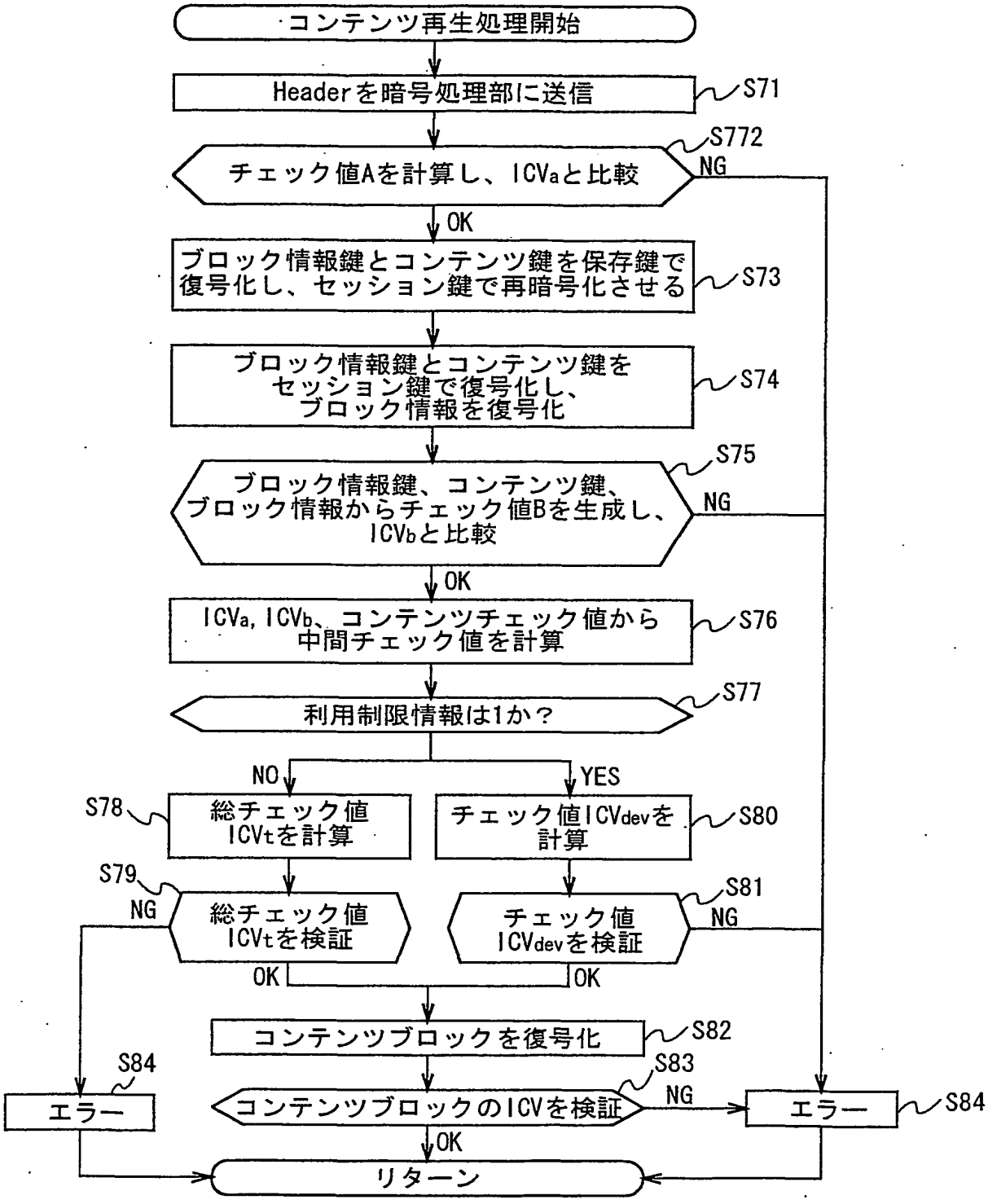

識別情報(Content ID)
取扱方針(Usage Policy)
チェック値A(ICVa)
ブロック情報秘鍵 (Kstr)
コンテンツ鍵 (Kcon)
ブロック情報(Block Information Table)
チェック値B(ICVb)
総チェック値 (ICVt)
コンテンツブロック1
コンテンツブロック2
コンテンツブロックi
コンテンツブロックN
Kstr
Kstr
Kbit
Kcon
Kcon
記録デバイスに保存されたコンテンツ
(記録制限情報 = 0)
暗号文データ
平文データ
署名データ

図26



記録デバイスに保存されたコンテンツ
(利用制限情報 = 1)

図27



コンテンツの再生処理

図２８

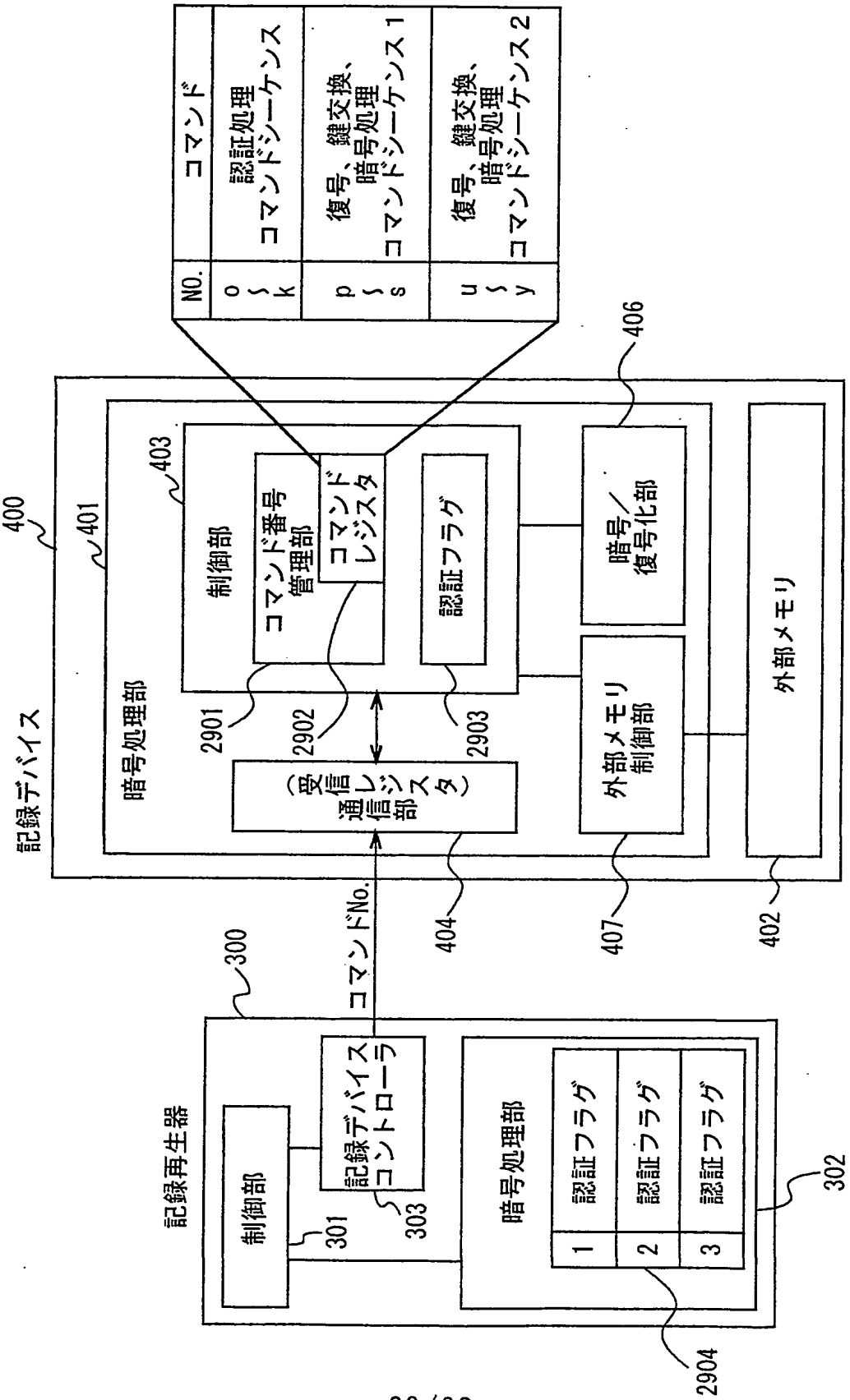

NO.
コマンド
o ～ k
認証処理 コマンドシーケンス
p ～ s
復号、鍵交換、暗号処理 コマンドシーケンス1
u ～ y
復号、鍵交換、暗号処理 コマンドシーケンス2
記録デバイス
400
401
暗号処理部
403
制御部
コマンド番号管理部
コマンドレジスタ
認証フラグ
406
暗号／復号化部
外部メモリ制御部
外部メモリ
2901
2902
2903
（受信レジスタ）通信部
404
407
402
コマンドNo.
300
記録再生器
制御部
301
記録デバイスコントローラ
303
暗号処理部
1 認証フラグ
2 認証フラグ
3 認証フラグ
302
2904

図２９

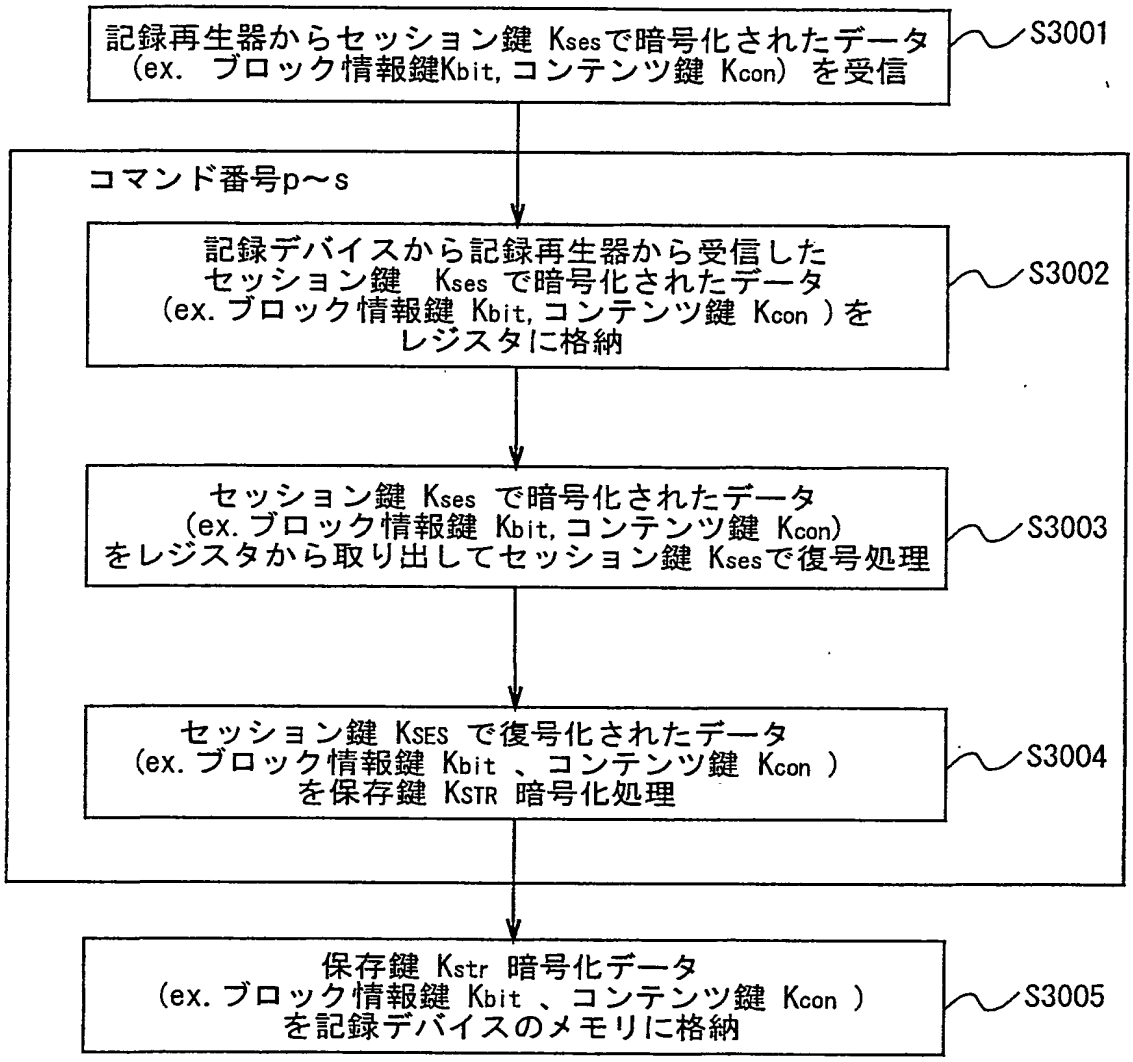

記録再生器からセッション鍵 Ksesで暗号化されたデータ
(ex. ブロック情報鍵Kbit, コンテンツ鍵 Kcon) を受信
S3001
コマンド番号p～s
記録デバイスから記録再生器から受信した
セッション鍵 Kses で暗号化されたデータ
(ex. ブロック情報鍵 Kbit, コンテンツ鍵 Kcon) を
レジスタに格納
S3002
セッション鍵 Kses で暗号化されたデータ
(ex. ブロック情報鍵 Kbit, コンテンツ鍵 Kcon)
をレジスタから取り出してセッション鍵 Ksesで復号処理
S3003
セッション鍵 KSES で復号化されたデータ
(ex. ブロック情報鍵 Kbit 、コンテンツ鍵 Kcon)
を保存鍵 KSTR 暗号化処理
S3004
保存鍵 Kstr 暗号化データ
(ex. ブロック情報鍵 Kbit 、コンテンツ鍵 Kcon)
を記録デバイスのメモリに格納
S3005

図３０

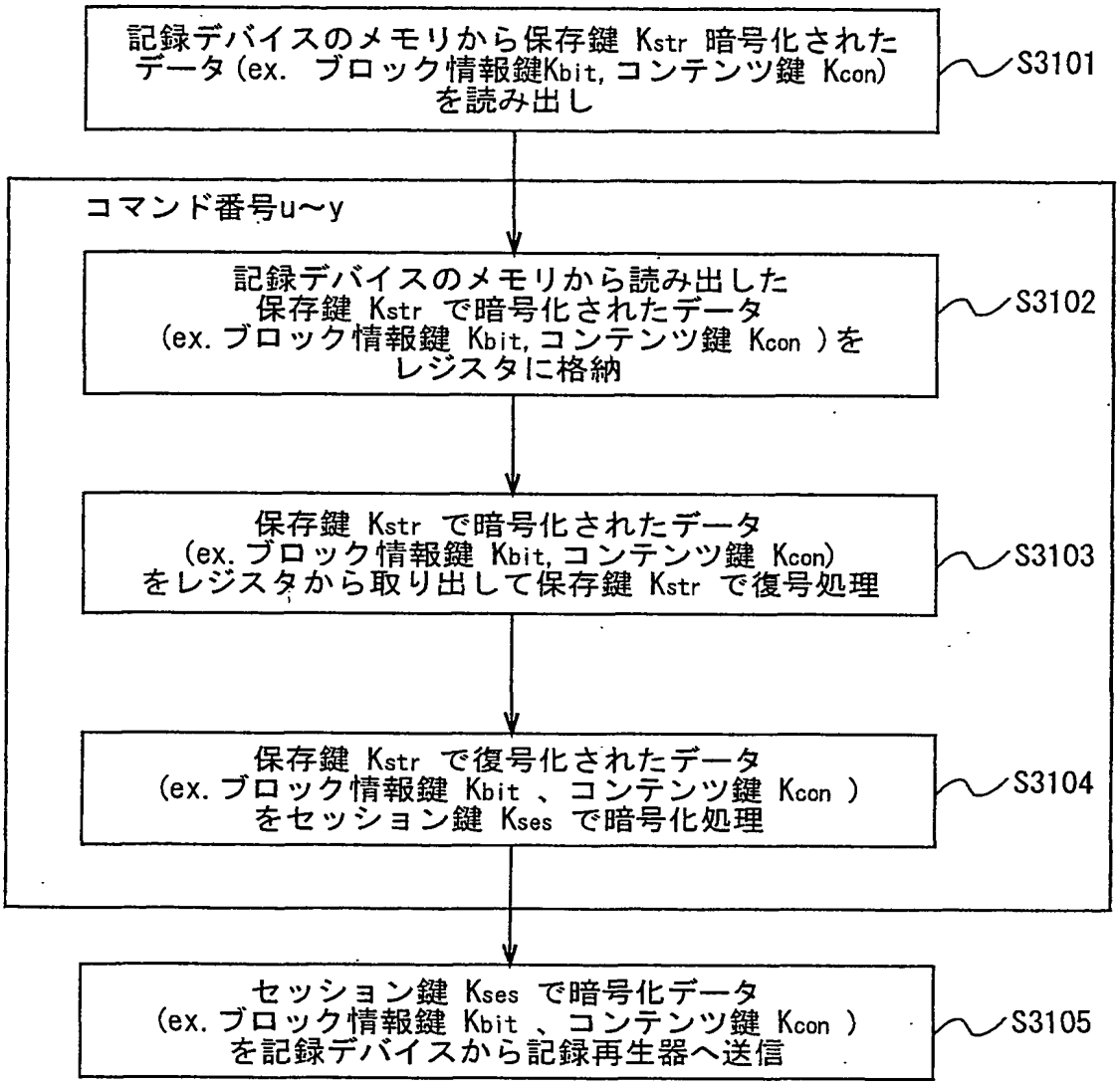
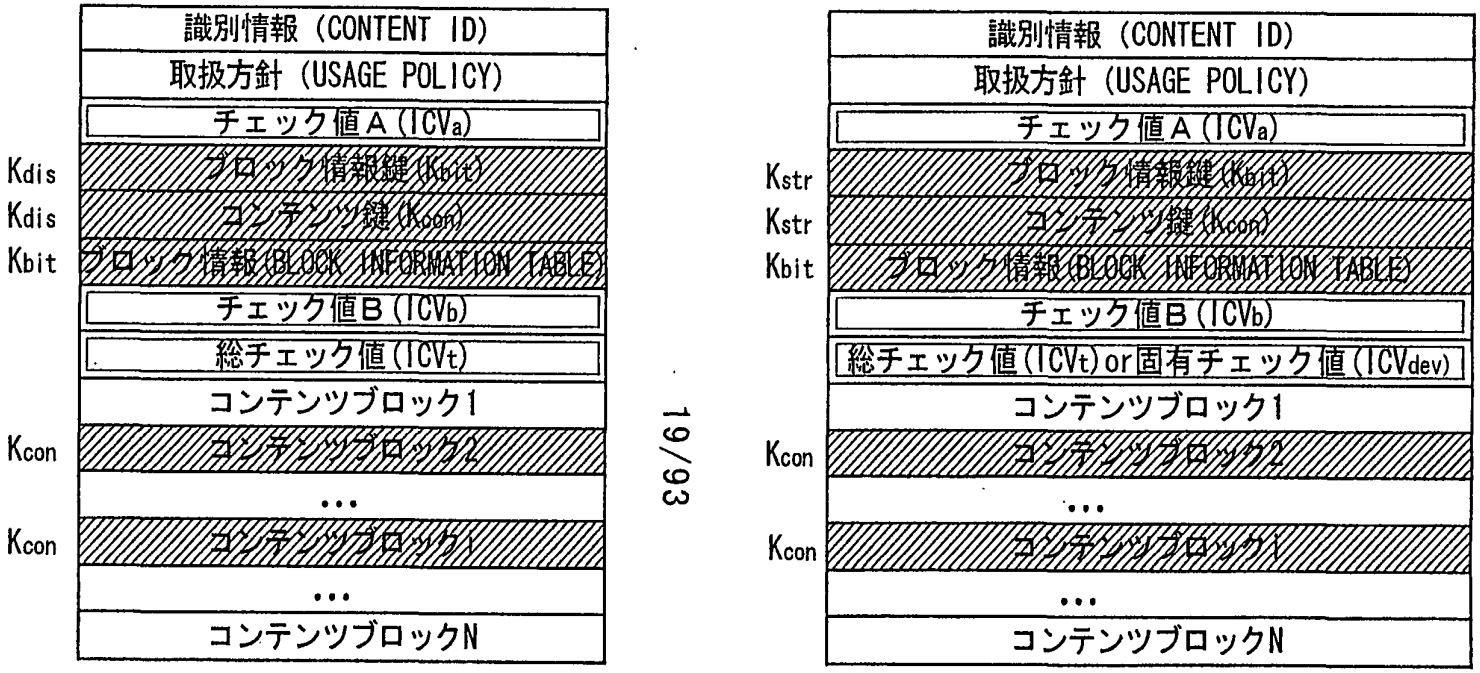

記録デバイスのメモリから保存鍵 Kstr 暗号化されたデータ(ex. ブロック情報鍵Kbit, コンテンツ鍵 Kcon)を読み出し
S3101
コマンド番号u~y
記録デバイスのメモリから読み出した保存鍵 Kstr で暗号化されたデータ(ex. ブロック情報鍵 Kbit, コンテンツ鍵 Kcon)をレジスタに格納
S3102
保存鍵 Kstr で暗号化されたデータ(ex. ブロック情報鍵 Kbit, コンテンツ鍵 Kcon)をレジスタから取り出して保存鍵 Kstr で復号処理
S3103
保存鍵 Kstr で復号化されたデータ(ex. ブロック情報鍵 Kbit 、コンテンツ鍵 Kcon)をセッション鍵 Kses で暗号化処理
S3104
セッション鍵 Kses で暗号化データ(ex. ブロック情報鍵 Kbit 、コンテンツ鍵 Kcon)を記録デバイスから記録再生器へ送信
S3105

図３１

フォーマット・タイプ０



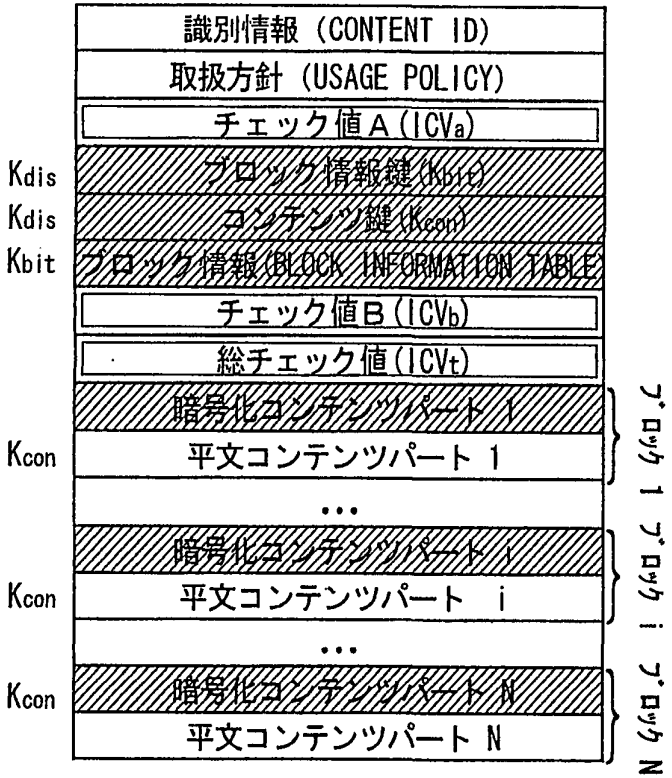
メディア上及び通信路上のデータフォーマット

記録デバイスに保存されたコンテンツ

暗号文データ　平文データ　署名データ

図３２

フォーマット・タイプ1



メディア上及び通信路上のデータフォーマット

記録デバイスに保存されたコンテンツ

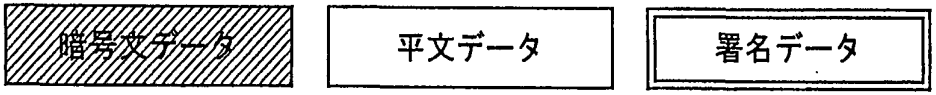
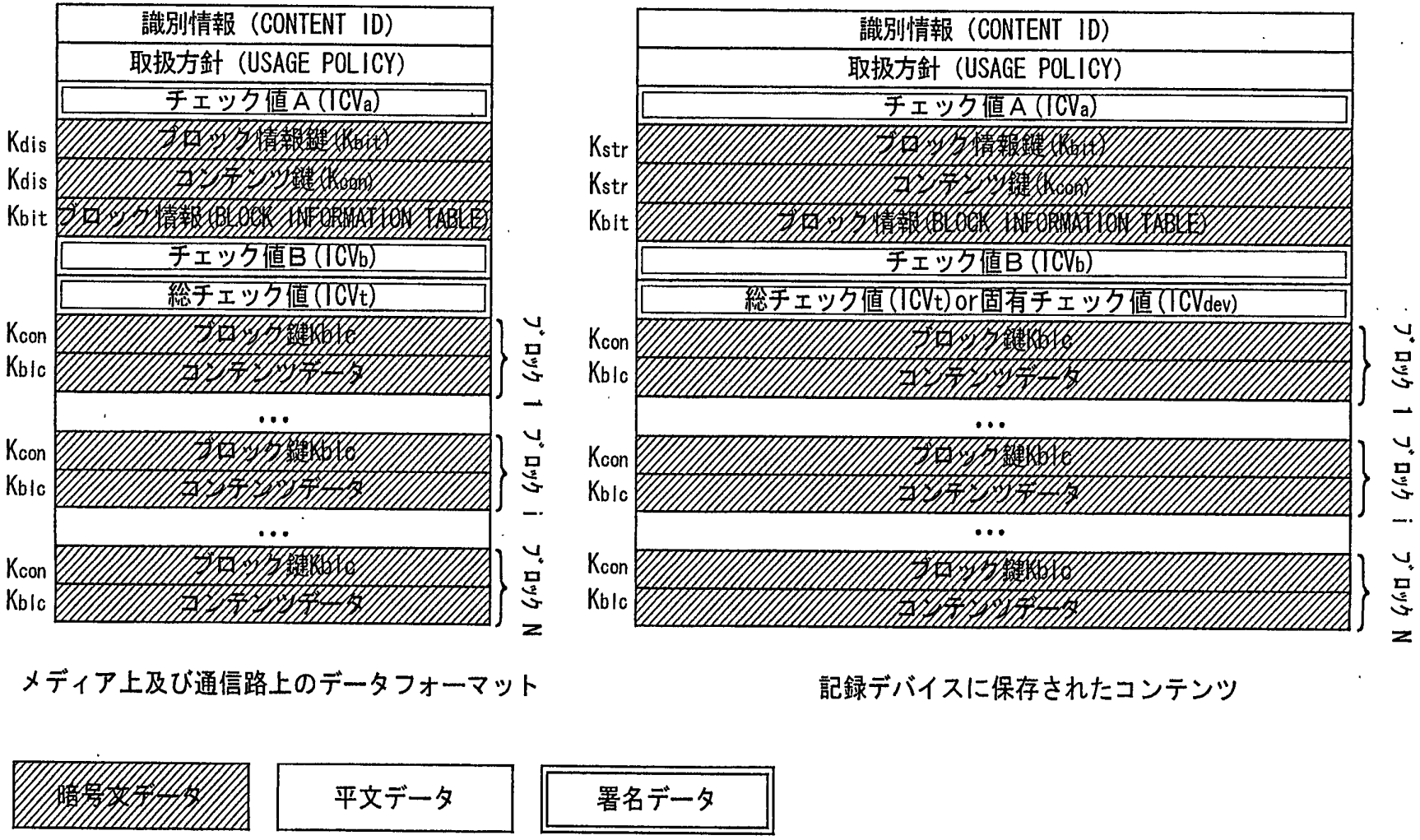


図３３

フォーマット・タイプ2



メディア上及び通信路上のデータフォーマット

記録デバイスに保存されたコンテンツ

暗号文データ　平文データ　署名データ

図34

フォーマット・タイプ3
識別情報 (CONTENT ID)
取扱方針 (USAGE POLICY)
チェック値A (ICVa)
ブロック情報鍵 (Kbit)
ブロック情報 (BLOCK INFORMATION TABLE)
チェック値B (ICVb)
総チェック値 (ICVt)
ブロック鍵Kblc
コンテンツデータ
Kdis
Kbit
Kstr
Kblc
ブロック 1
ブロック i
ブロック N
メディア上及び通信路上のデータフォーマット
総チェック値 (ICVt) or 固有チェック値 (ICVdev)
記録デバイスに保存されたコンテンツ
暗号文データ
平文データ
署名データ

図35

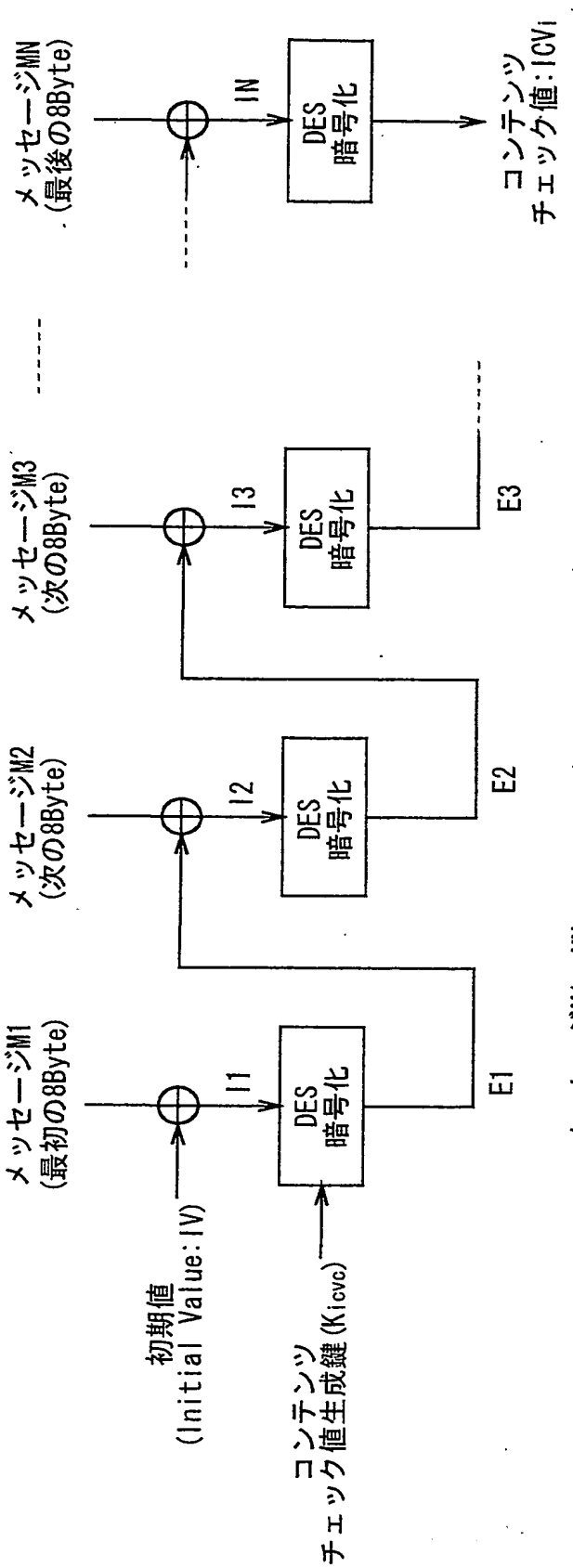

メッセージM1
(最初の8Byte)
メッセージM2
(次の8Byte)
メッセージM3
(次の8Byte)
メッセージMN
(最後の8Byte)
初期値
(Initial Value:IV)
コンテンツ
チェック値生成鍵(Kicvc)
I1
I2
I3
IN
DES
暗号化
E1
E2
E3
コンテンツ
チェック値:ICVi
メッセージM1～MN:コンテンツiのコンテンツデータ
⊕:排他的論理和処理(8バイト単位)

図３６

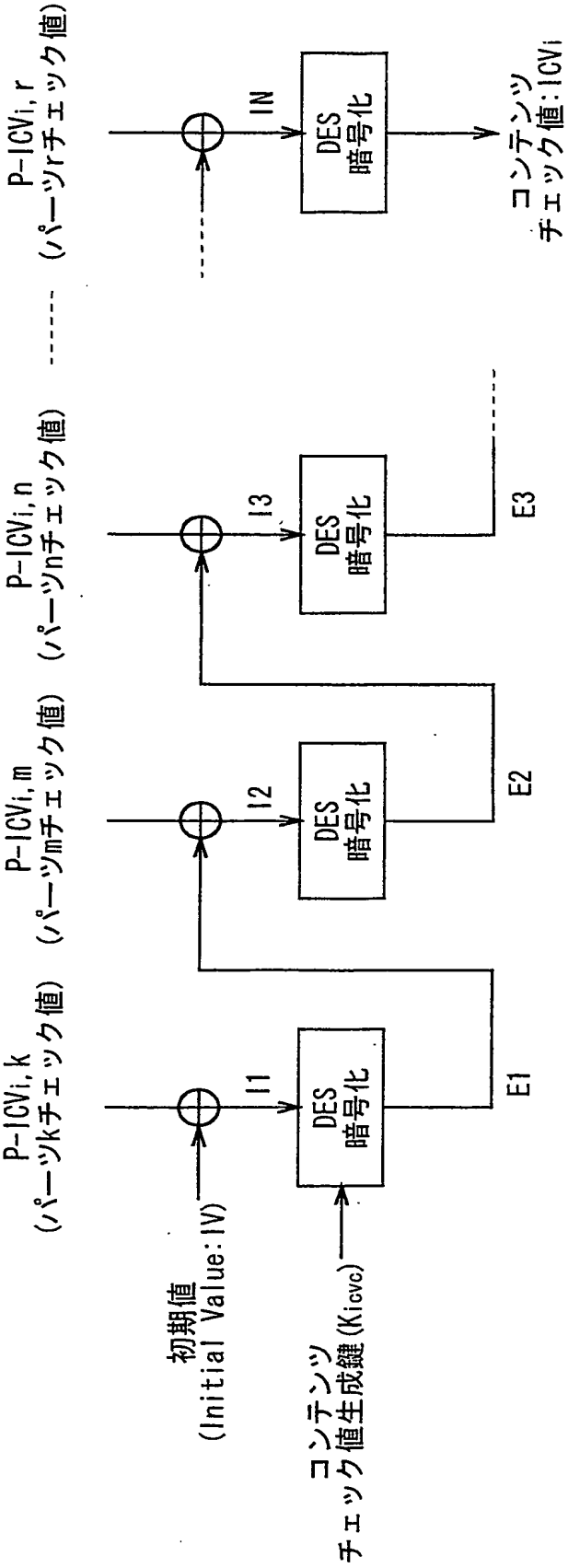
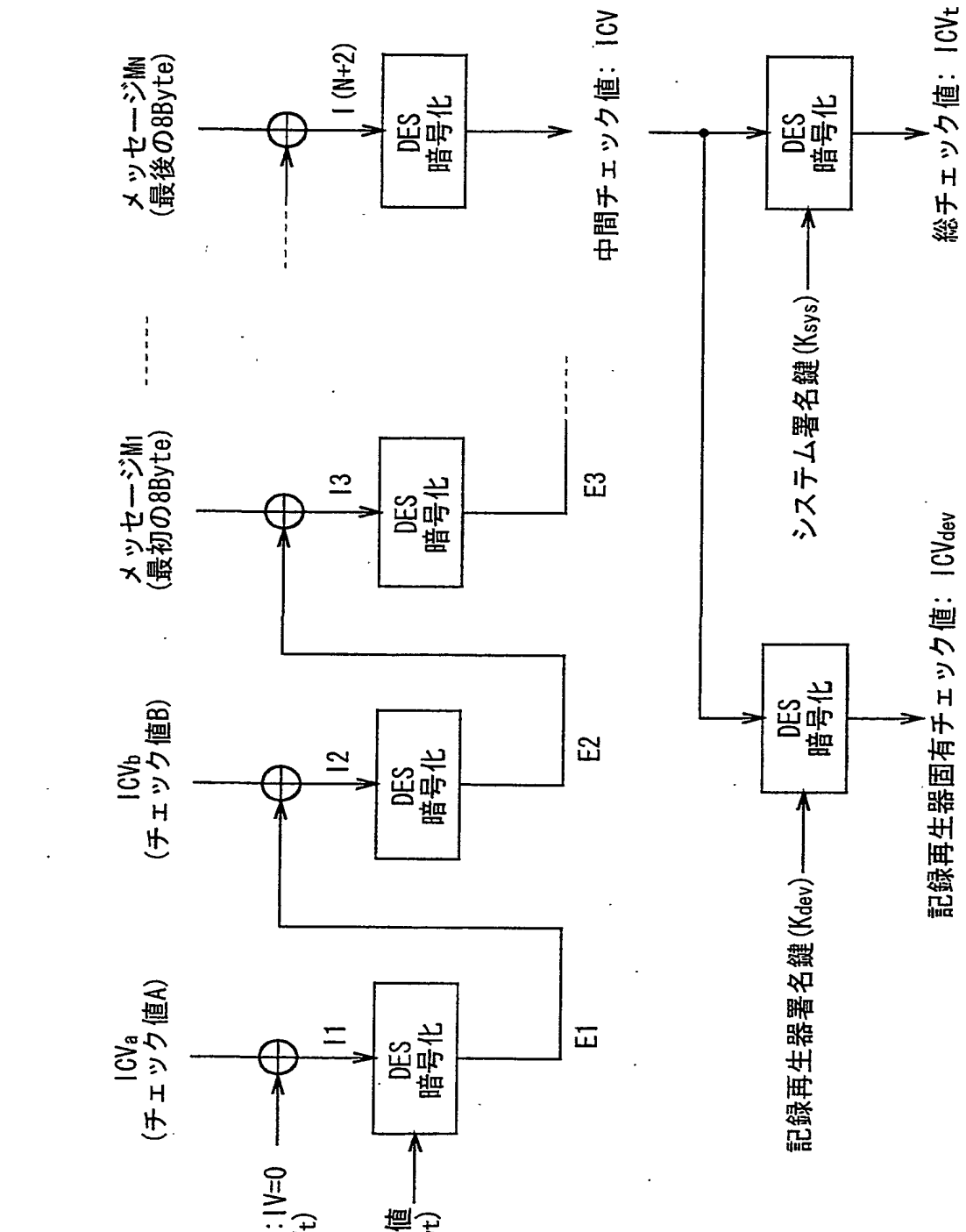

P-ICVi, k
(パーツkチェック値)
P-ICVi, m
(パーツmチェック値)
P-ICVi, n
(パーツnチェック値)
P-ICVi, r
(パーツrチェック値)
初期値
(Initial Value: IV)
コンテンツ
チェック値生成鍵 (Kicvc)
I1
I2
I3
IN
DES
暗号化
E1
E2
E3
コンテンツ
チェック値: ICVi
⊕:排他的論理和処理 (8バイト単位)

図３７



メッセージM1～MN:コンテンツブロック1～Nのデータ

⊕:排他的論理和処理(8バイト単位)

図３８

フォーマットタイプ０，１ダウンロード処理

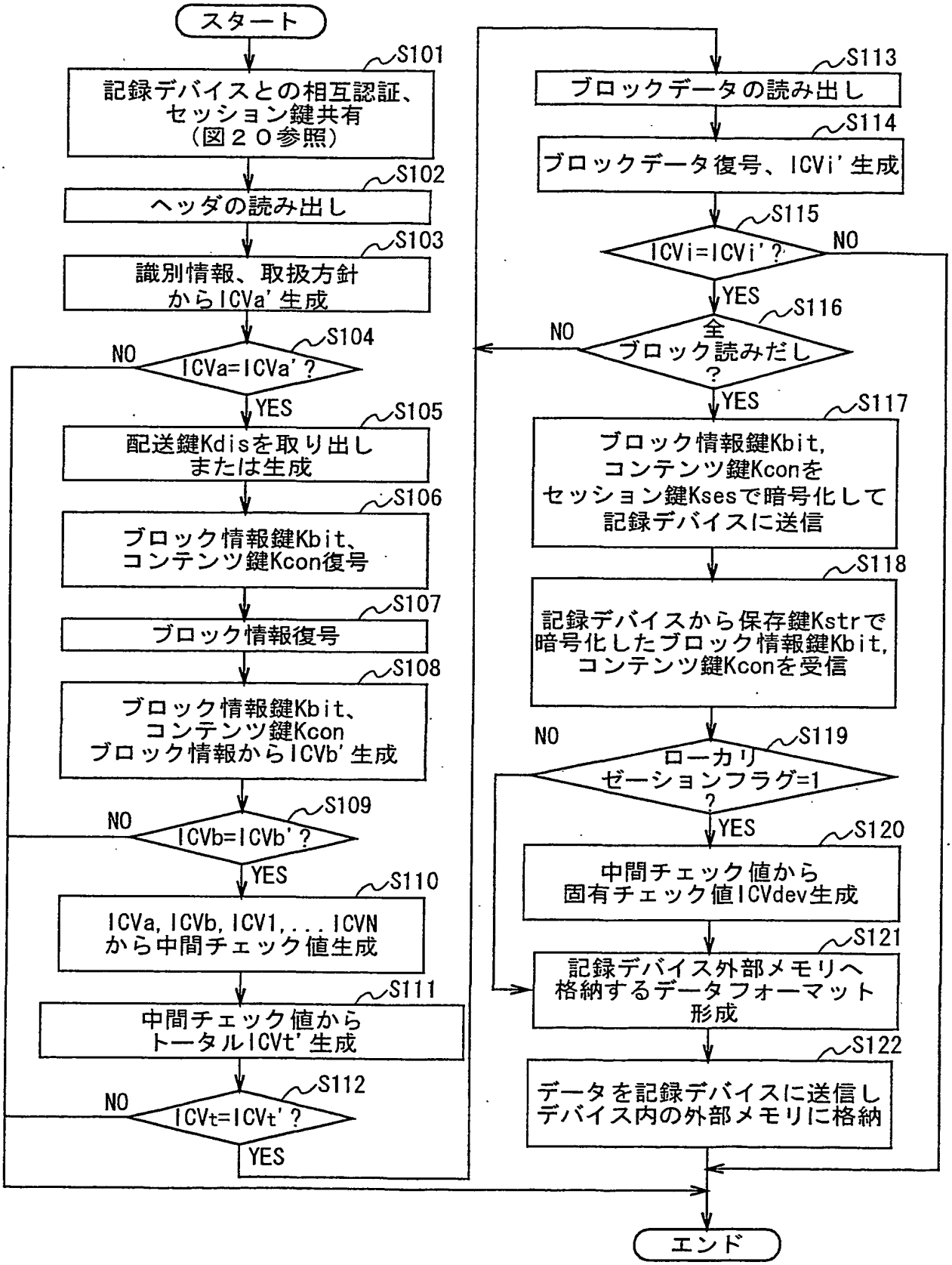


図３９

フォーマットタイプ２ダウンロード処理

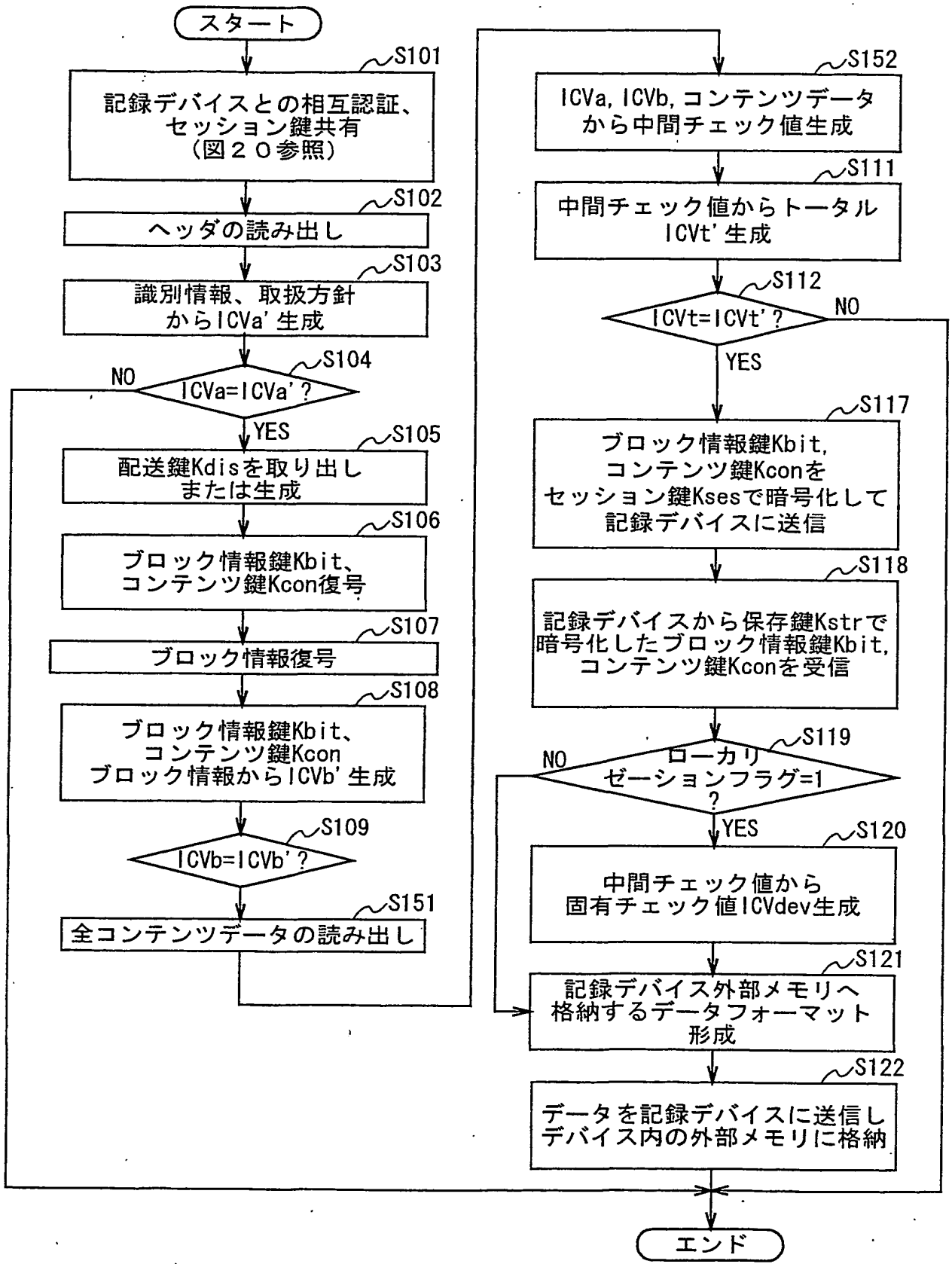


図４０

フォーマットタイプ３ダウンロード処理

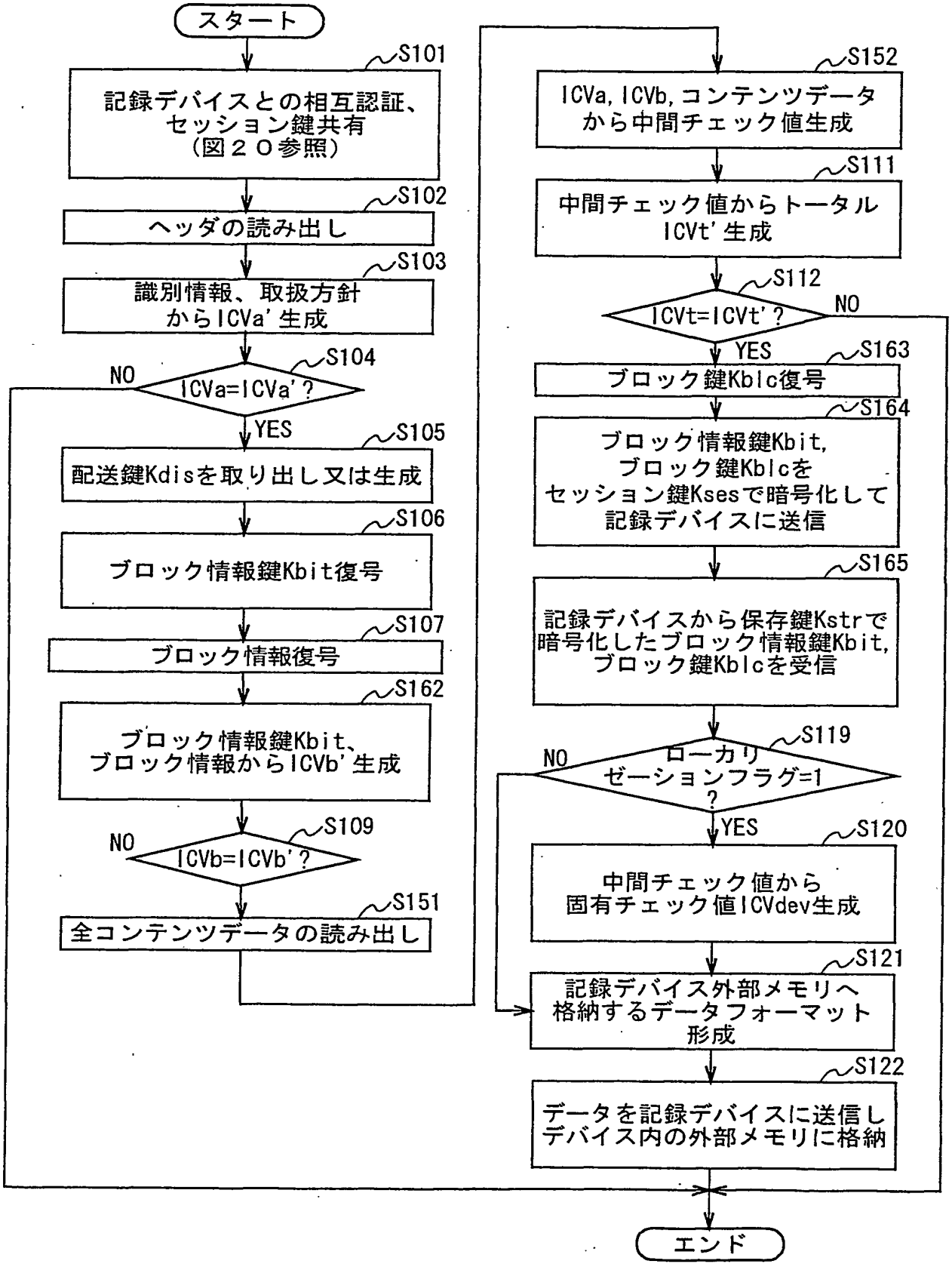


図４１

フォーマットタイプ０再生処理

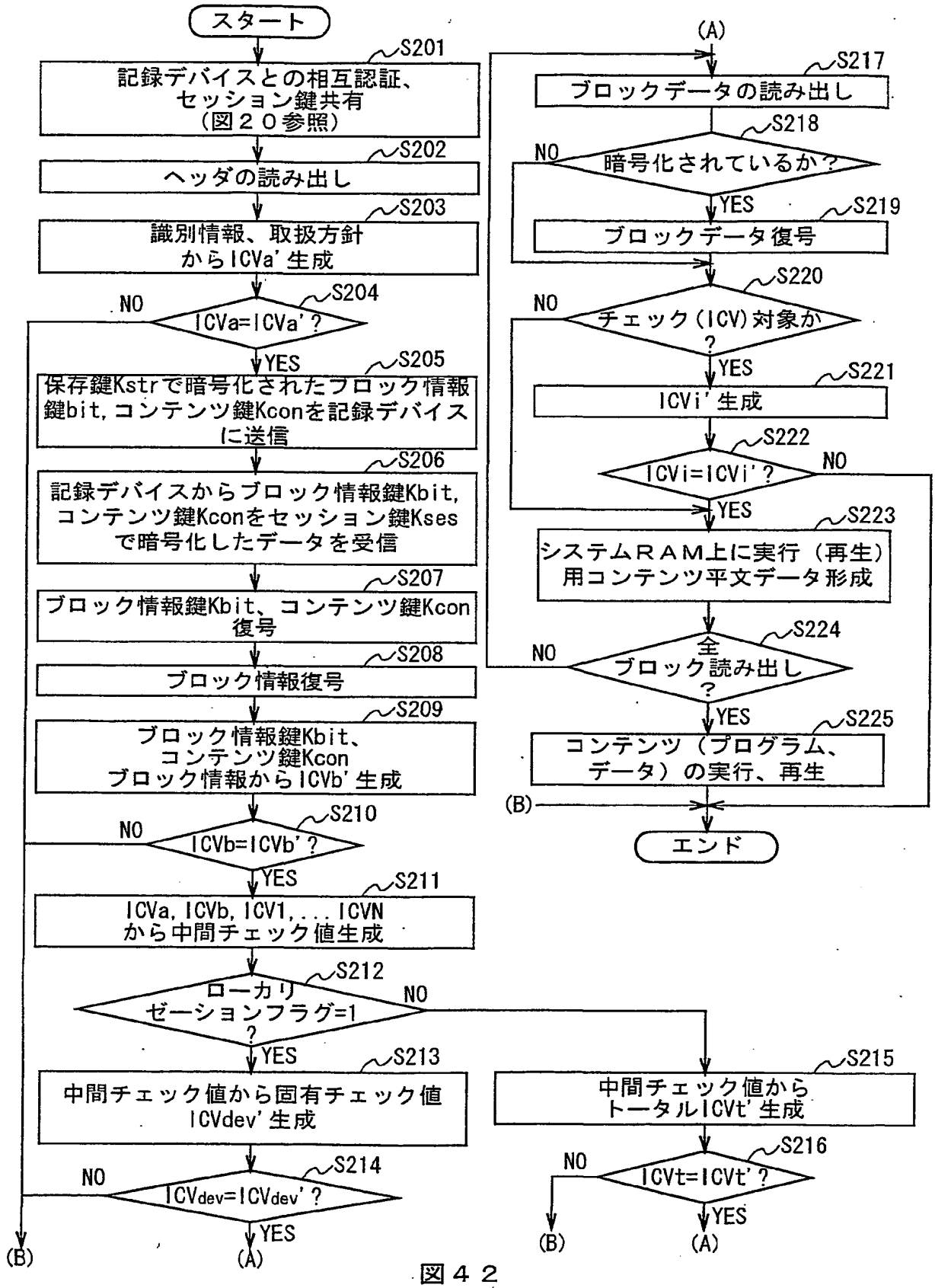


図４２

フォーマットタイプ１再生処理

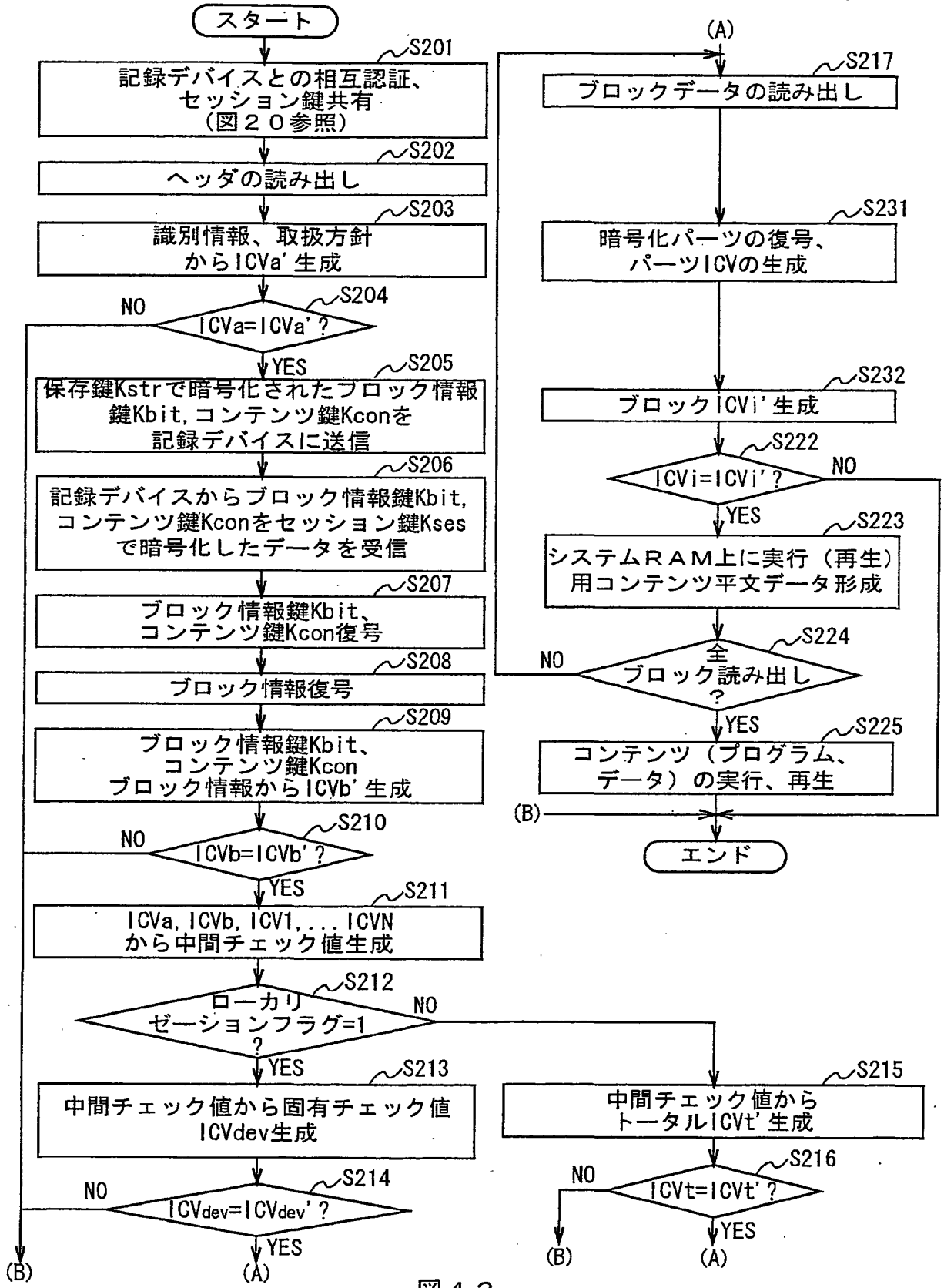


図４３

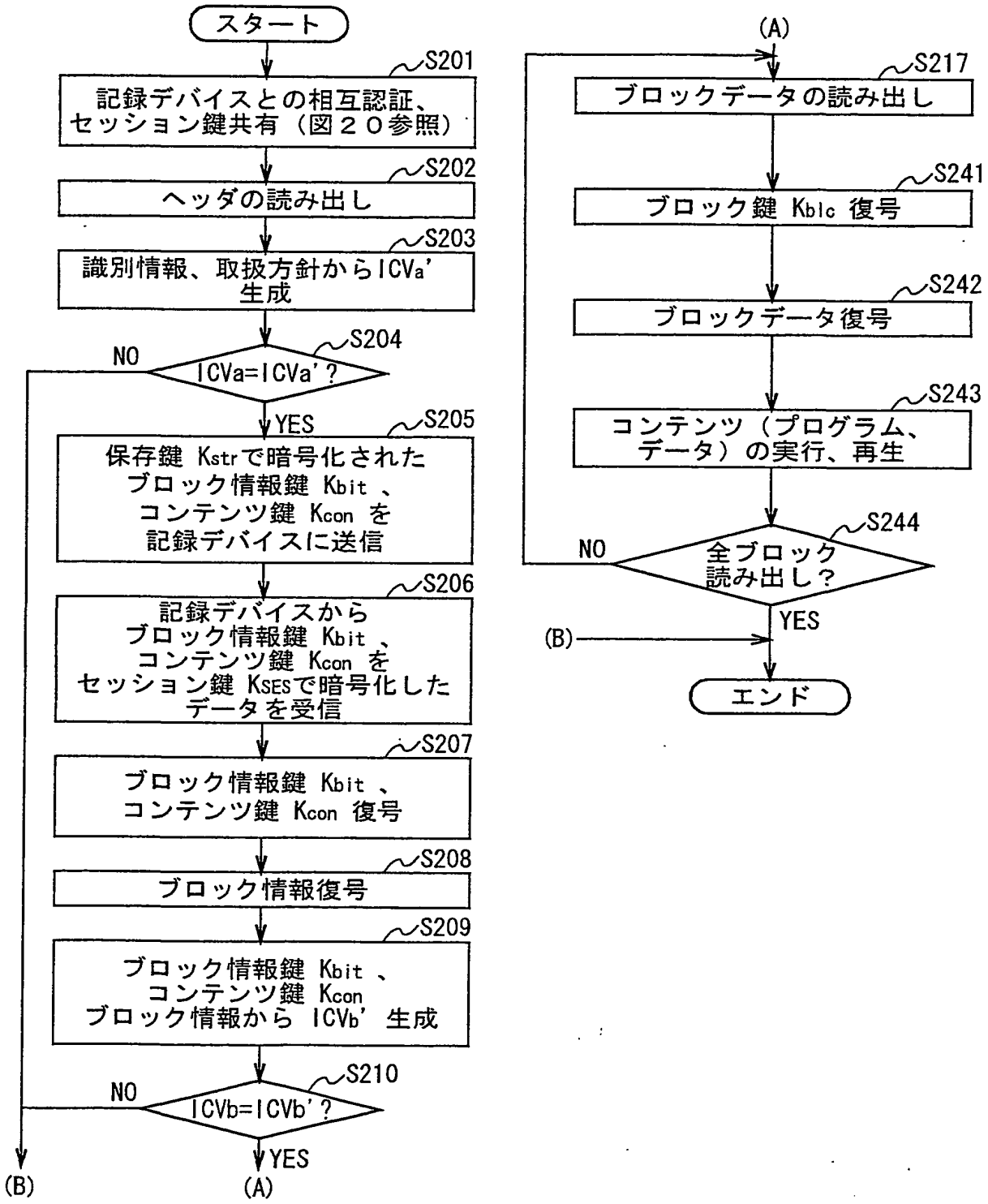

スタート
S201
記録デバイスとの相互認証、セッション鍵共有（図２０参照）
S202
ヘッダの読み出し
S203
識別情報、取扱方針からICVa'生成
S204
NO
ICVa=ICVa'？
YES
S205
保存鍵 Kstrで暗号化されたブロック情報鍵 Kbit 、コンテンツ鍵 Kcon を記録デバイスに送信
S206
記録デバイスからブロック情報鍵 Kbit 、コンテンツ鍵 Kcon をセッション鍵 KSESで暗号化したデータを受信
S207
ブロック情報鍵 Kbit 、コンテンツ鍵 Kcon 復号
S208
ブロック情報復号
S209
ブロック情報鍵 Kbit 、コンテンツ鍵 Kcon ブロック情報から ICVb' 生成
S210
NO
ICVb=ICVb'？
YES
(B)
(A)
(A)
S217
ブロックデータの読み出し
S241
ブロック鍵 Kblc 復号
S242
ブロックデータ復号
S243
コンテンツ（プログラム、データ）の実行、再生
S244
NO
全ブロック読み出し？
YES
(B)
エンド

図４４

フォーマットタイプ3再生処理

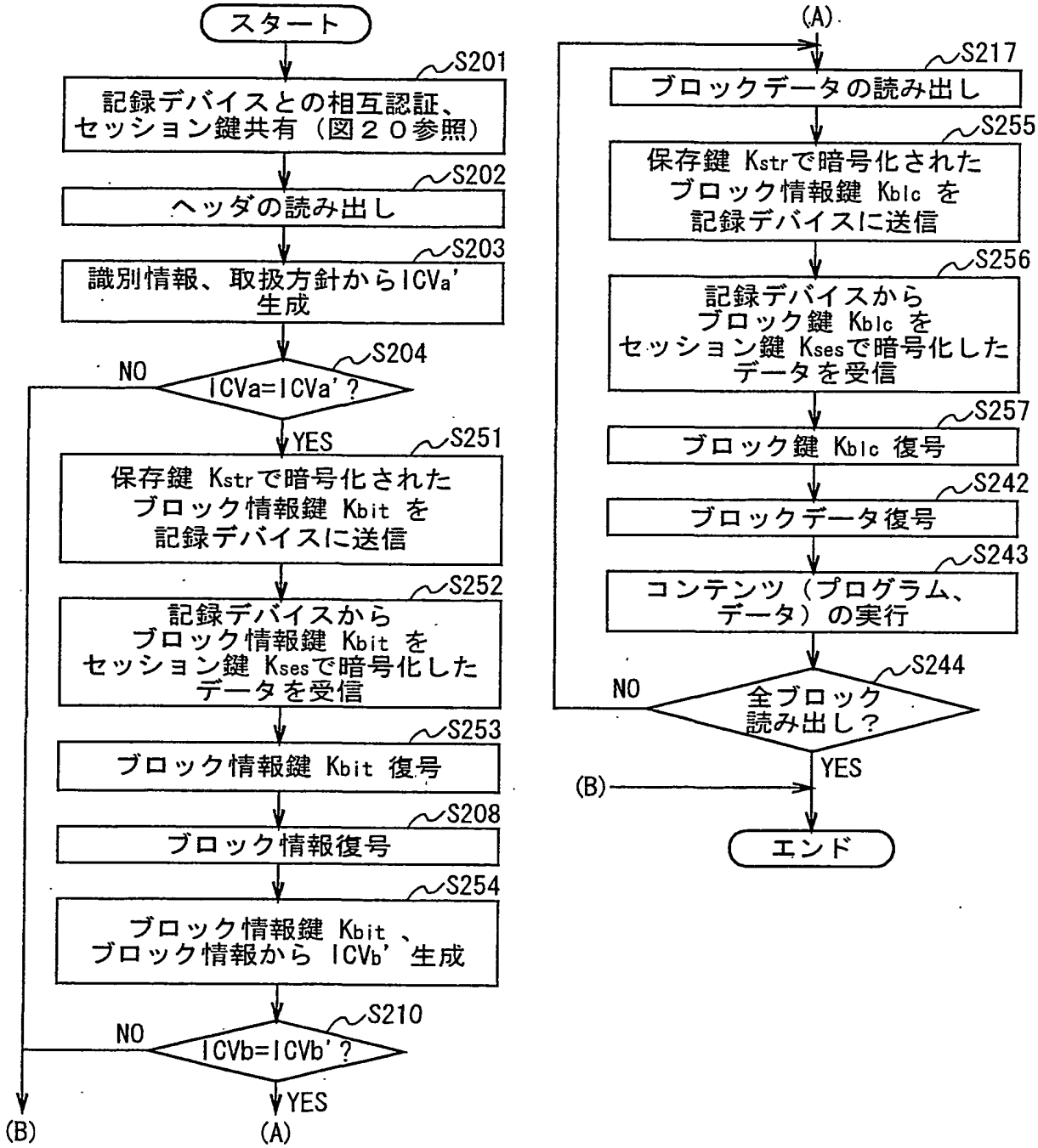


図４５

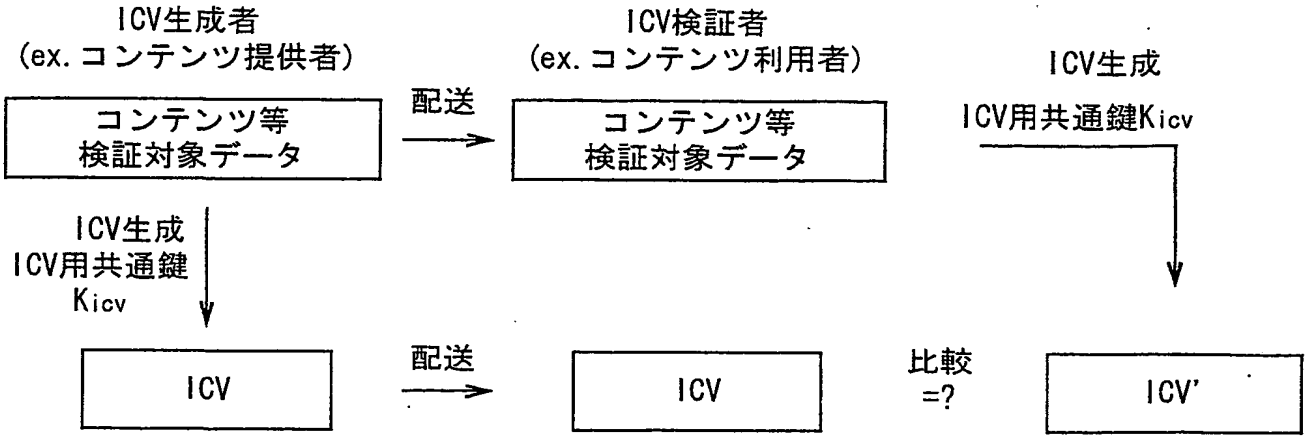

ICV生成者
(ex. コンテンツ提供者)
ICV検証者
(ex. コンテンツ利用者)
ICV生成
ICV用共通鍵Kicv
コンテンツ等
検証対象データ
配送
コンテンツ等
検証対象データ
ICV生成
ICV用共通鍵
Kicv
ICV
配送
ICV
比較
=?
ICV'

図４６

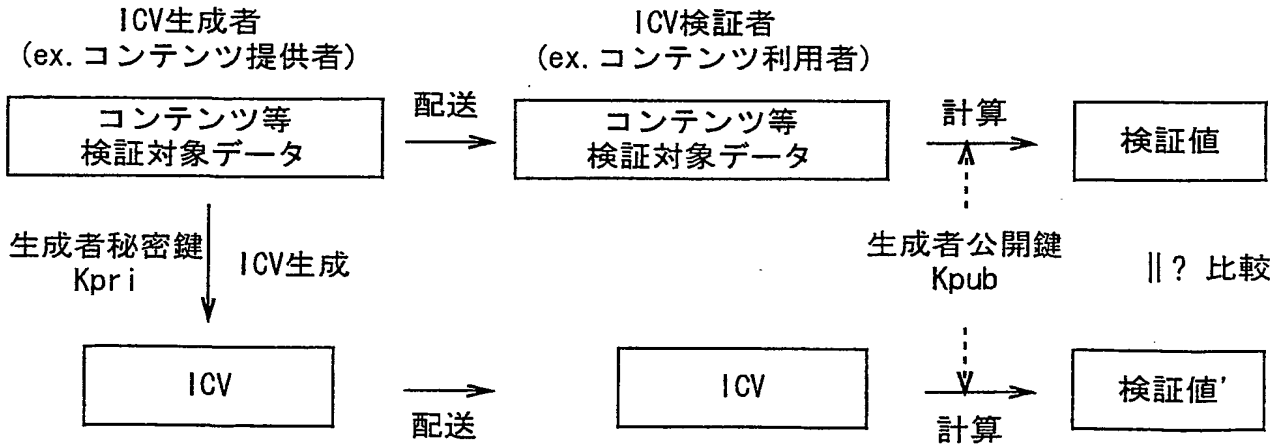

ICV生成者
(ex. コンテンツ提供者)
ICV検証者
(ex. コンテンツ利用者)
コンテンツ等
検証対象データ
配送
コンテンツ等
検証対象データ
計算
検証値
生成者秘密鍵
Kpri
ICV生成
生成者公開鍵
Kpub
||? 比較
ICV
配送
ICV
計算
検証値'

図４７

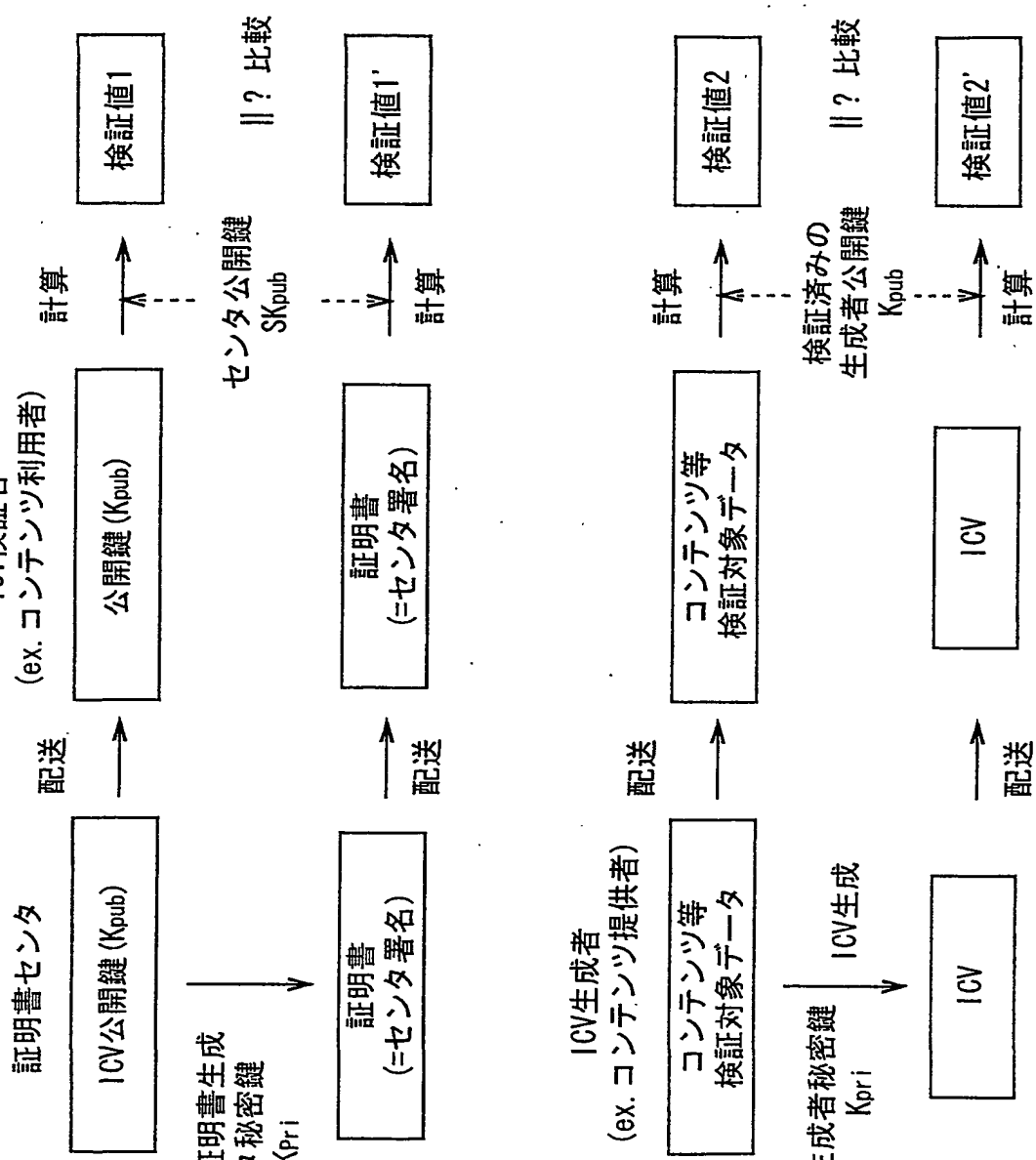

証明書センタ
ICV公開鍵 (Kpub)
配送
ICV検証者
(ex. コンテンツ利用者)
公開鍵 (Kpub)
計算
検証値1
センタ公開鍵
SKpub
||? 比較
公開鍵証明書生成
センタ秘密鍵
SKPri
証明書
(=センタ署名)
配送
証明書
(=センタ署名)
計算
検証値1'
ICV生成者
(ex. コンテンツ提供者)
コンテンツ等
検証対象データ
配送
コンテンツ等
検証対象データ
計算
検証値2
検証済みの
生成者公開鍵
Kpub
||? 比較
生成者秘密鍵
Kpri
ICV生成
ICV
配送
ICV
計算
検証値2'

図48

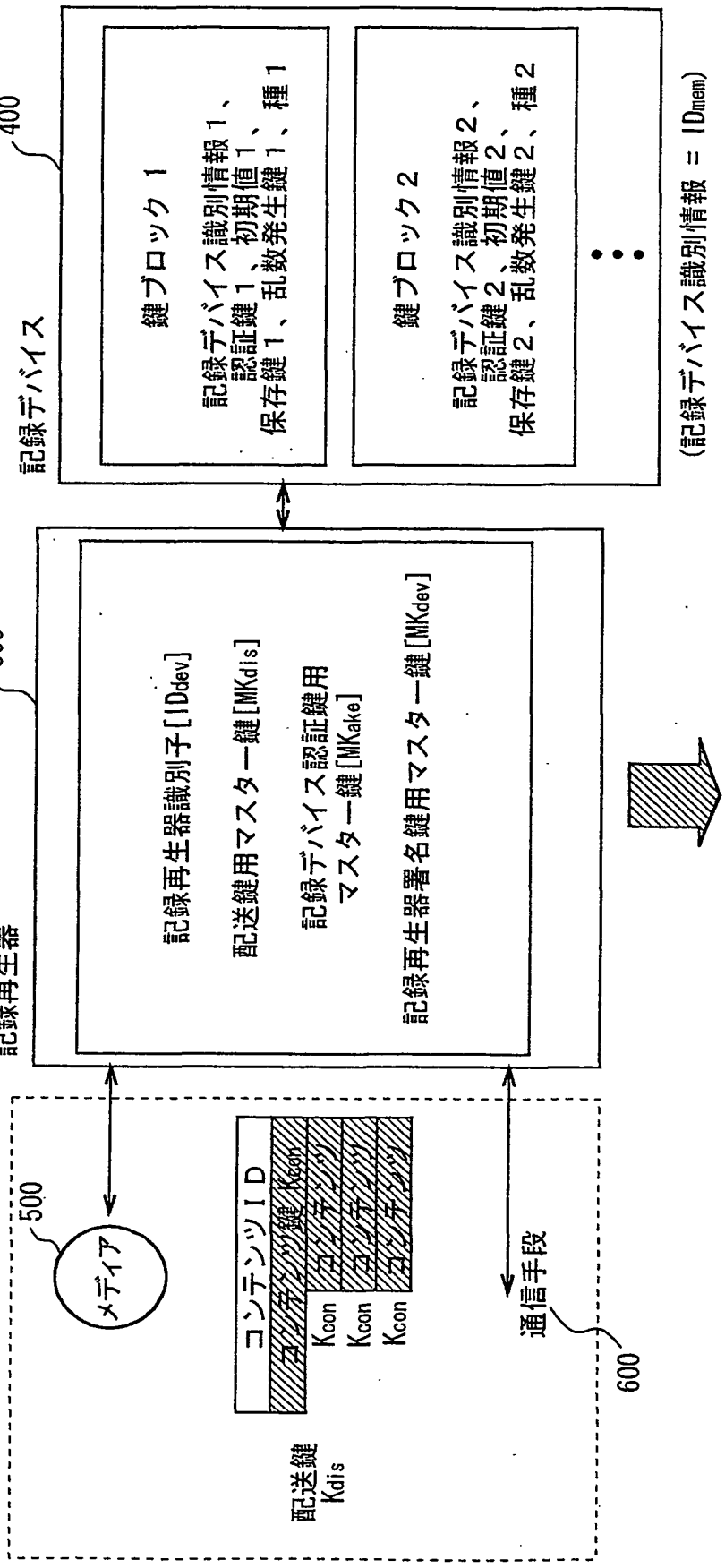
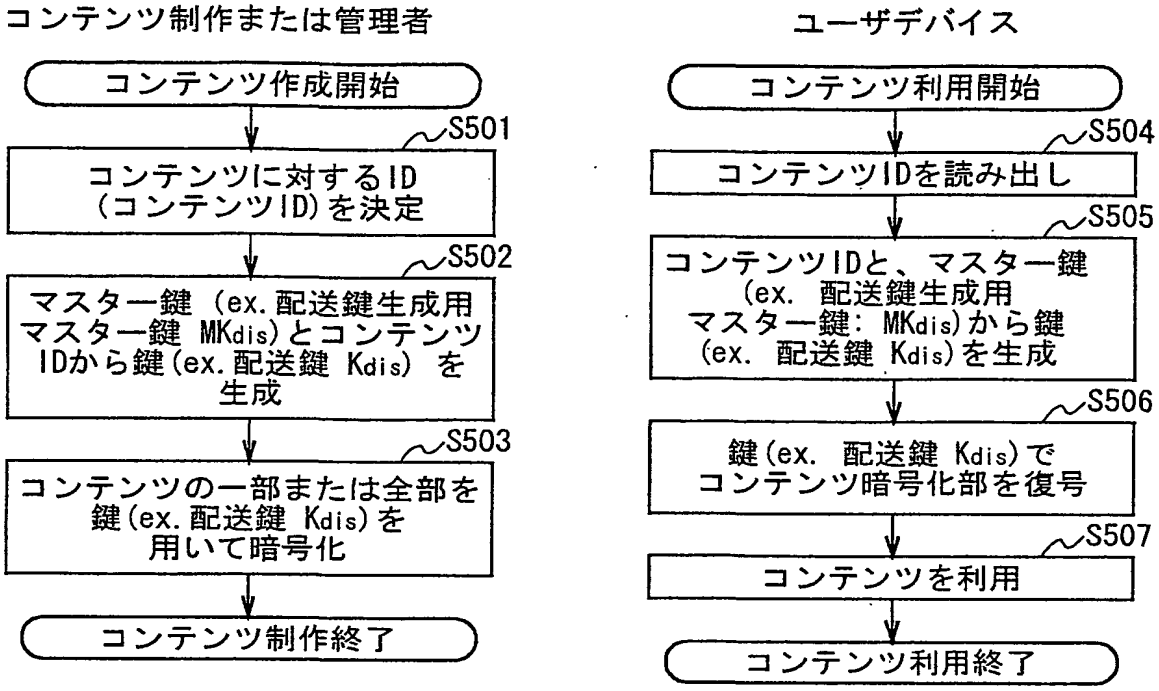

記録デバイス
400
鍵ブロック１
記録デバイス識別情報１、
認証鍵１、初期値１、
保存鍵１、乱数発生鍵１、種１
鍵ブロック２
記録デバイス識別情報２、
認証鍵２、初期値２、
保存鍵２、乱数発生鍵２、種２
(記録デバイス識別情報 = IDmem)
記録再生器
300
記録再生器識別子[IDdev]
配送鍵用マスター鍵[MKdis]
記録デバイス認証鍵用
マスター鍵[MKake]
記録再生器署名鍵用マスター鍵[MKdev]
メディア
500
コンテンツＩＤ
コンテンツ鍵 Kcon
コンテンツ
Kcon
コンテンツ
Kcon
配送鍵
Kdis
通信手段
600
配送鍵 : Kdis = DES (MKdis, コンテンツＩＤ)
認証鍵 : Kake = DES (MKake, IDmem)
記録再生器署名鍵 : Kdev = DES (MKdev, IDdev)

図４９

Master鍵から個別の鍵を生成する方法ー(1)

[基本フロー]



[鍵所有構成]

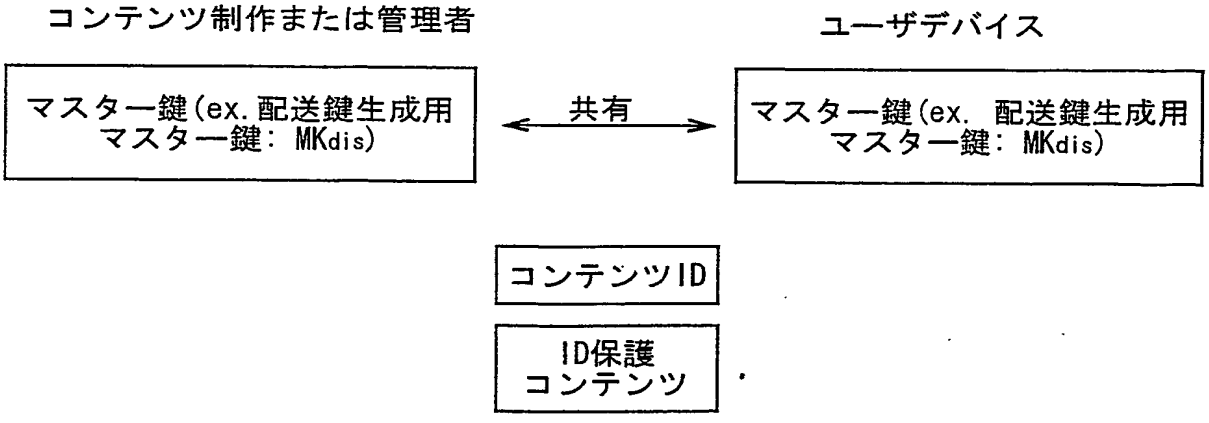
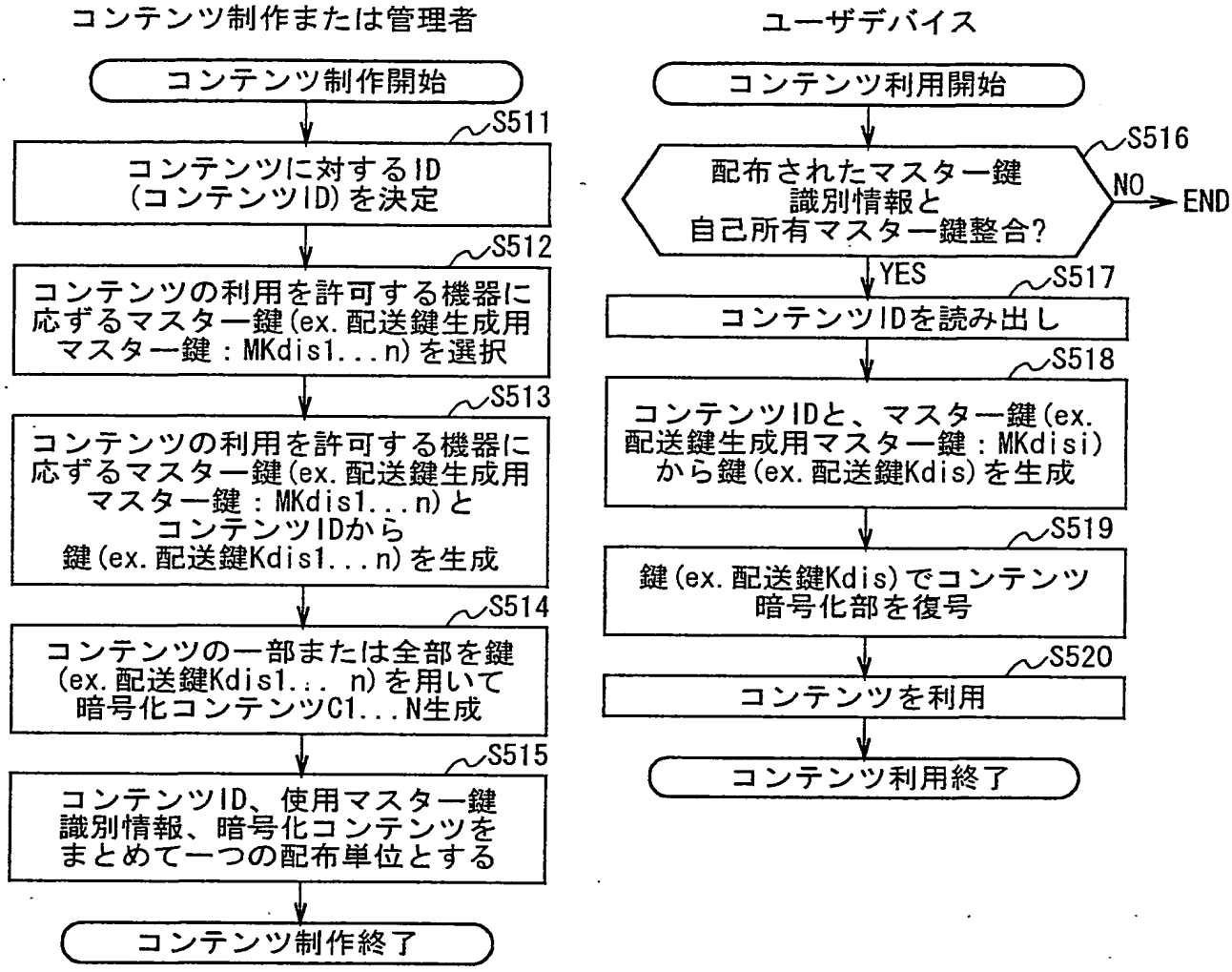


図５０

Master鍵から個別の鍵を生成する方法-(2)

[基本フロー]



[鍵所有構成]

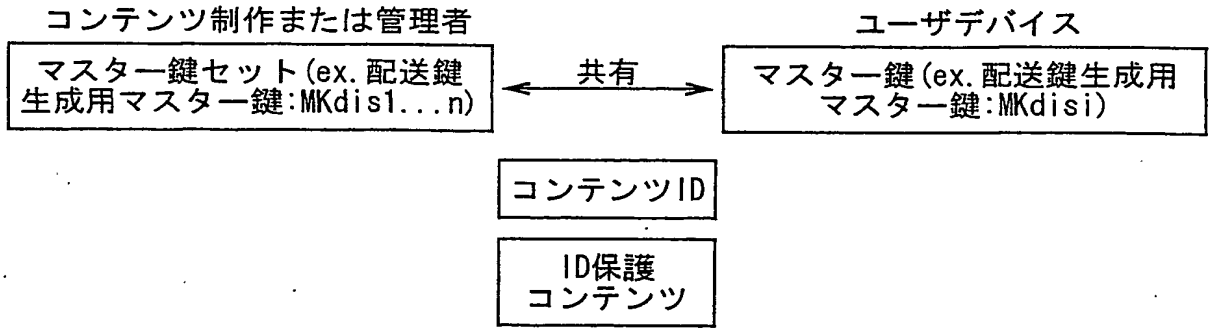


図５１

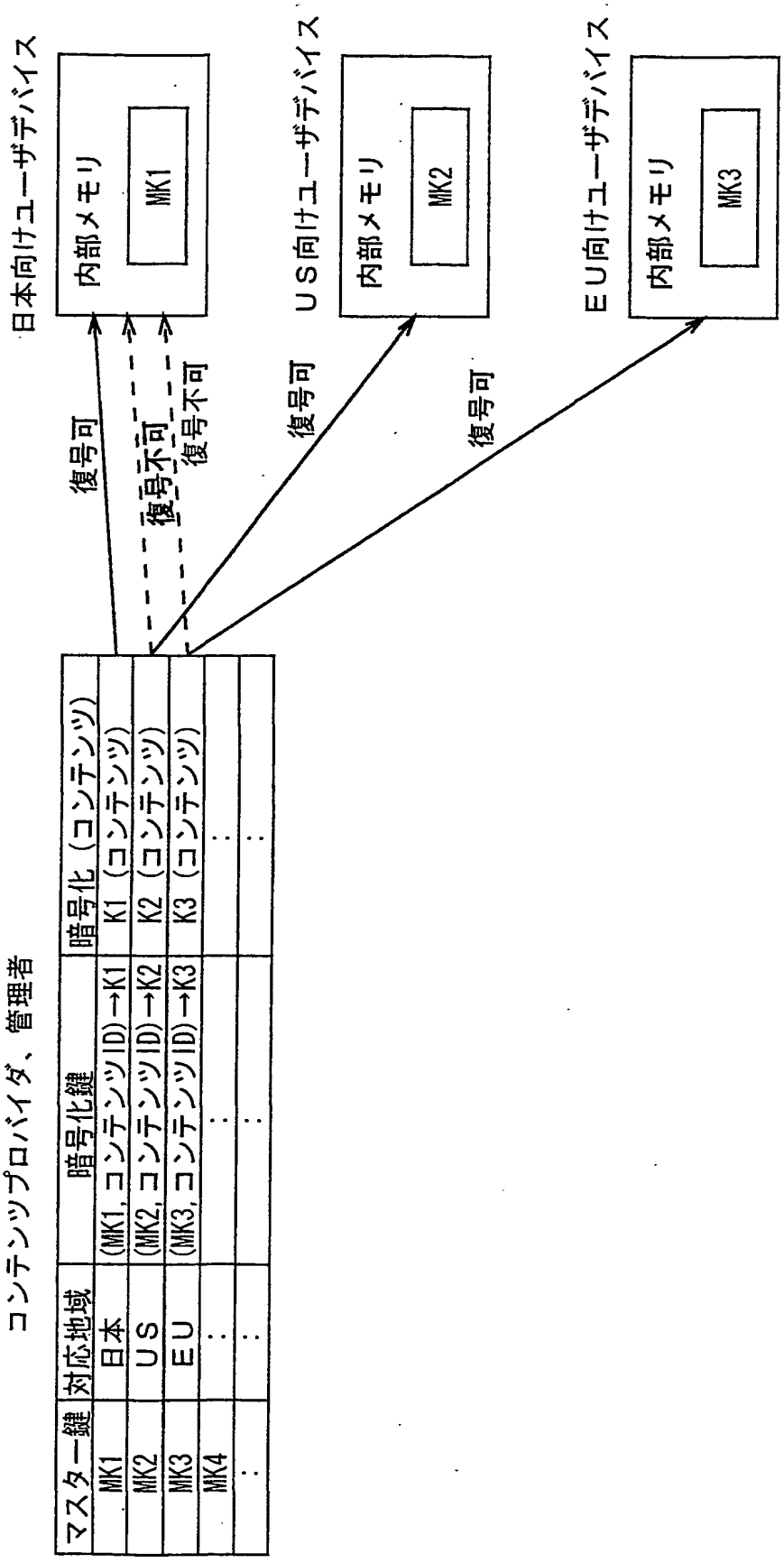
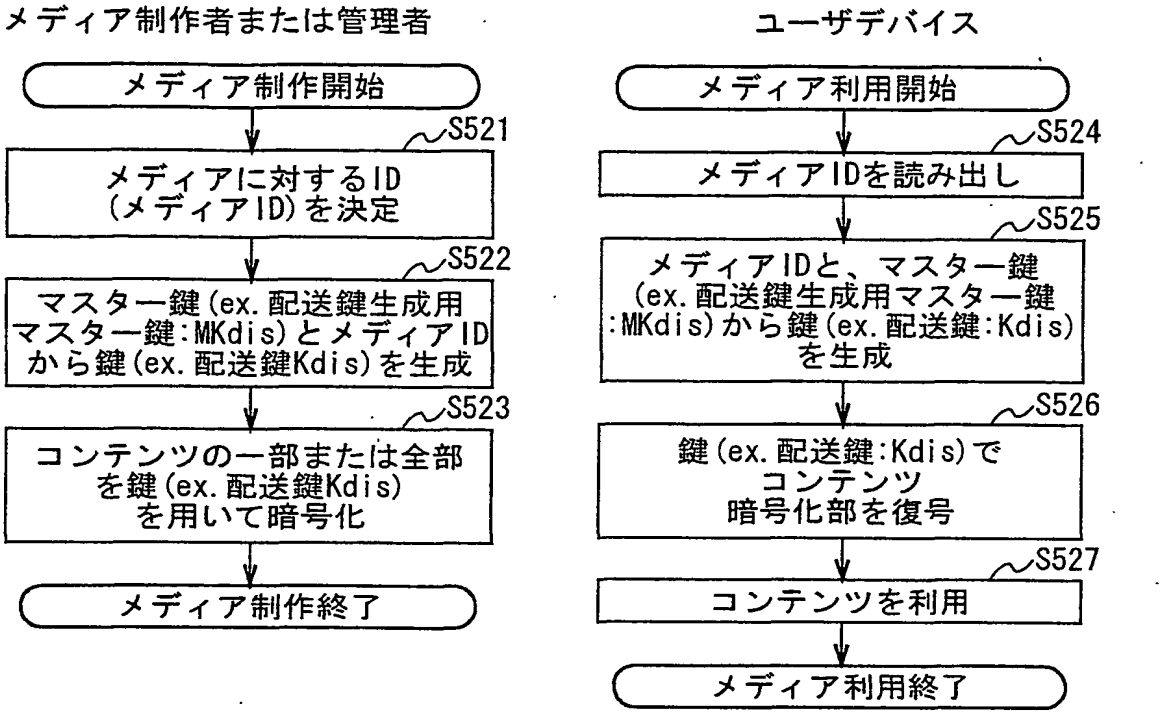

日本向けユーザデバイス
内部メモリ
MK1
US向けユーザデバイス
内部メモリ
MK2
EU向けユーザデバイス
内部メモリ
MK3
復号可
復号不可
復号不可
復号可
復号可
コンテンツプロバイダ、管理者
マスター鍵
対応地域
暗号化鍵
暗号化（コンテンツ）
MK1
日本
(MK1, コンテンツID)→K1
K1（コンテンツ）
MK2
US
(MK2, コンテンツID)→K2
K2（コンテンツ）
MK3
EU
(MK3, コンテンツID)→K3
K3（コンテンツ）
MK4

図52

Master鍵から個別の鍵を生成する方法-(3)

[基本フロー]



[鍵所有構成]

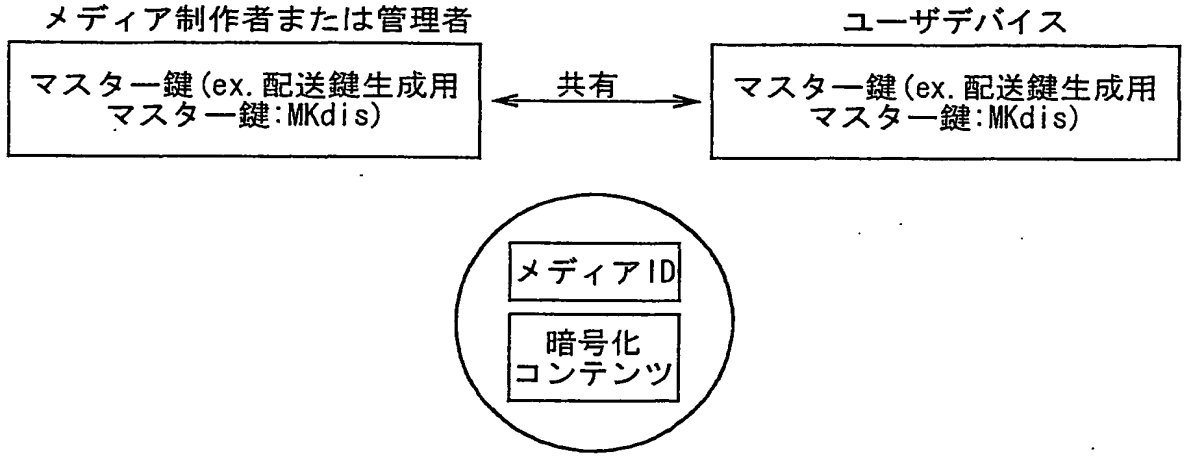
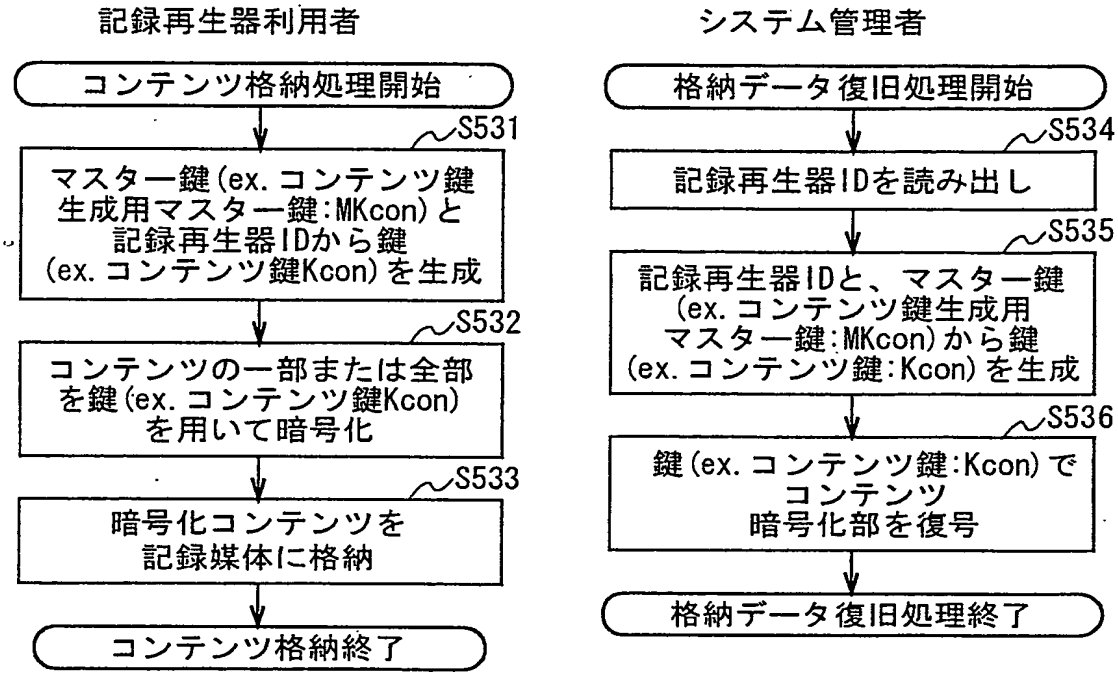


図５３

Master鍵から個別の鍵を生成する方法－(4)

[基本フロー]



[鍵所有構成]

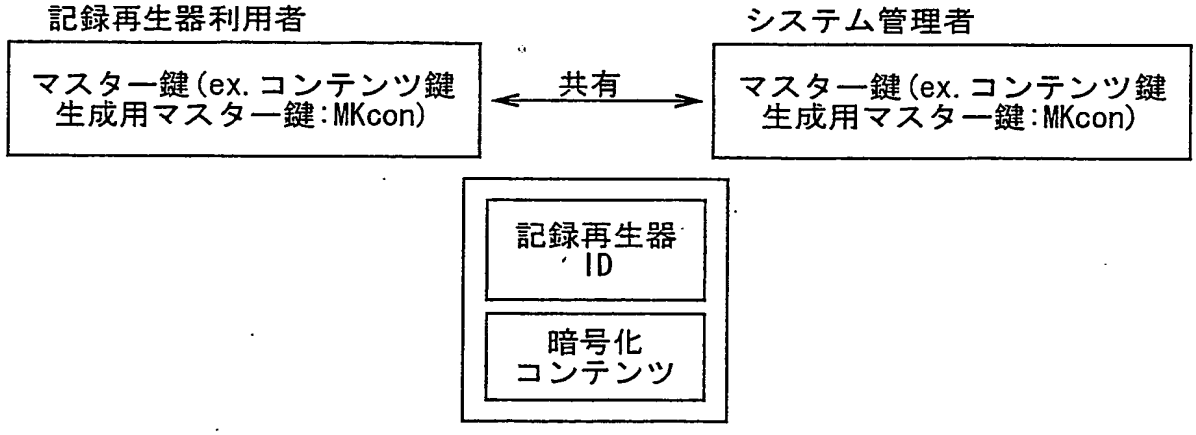
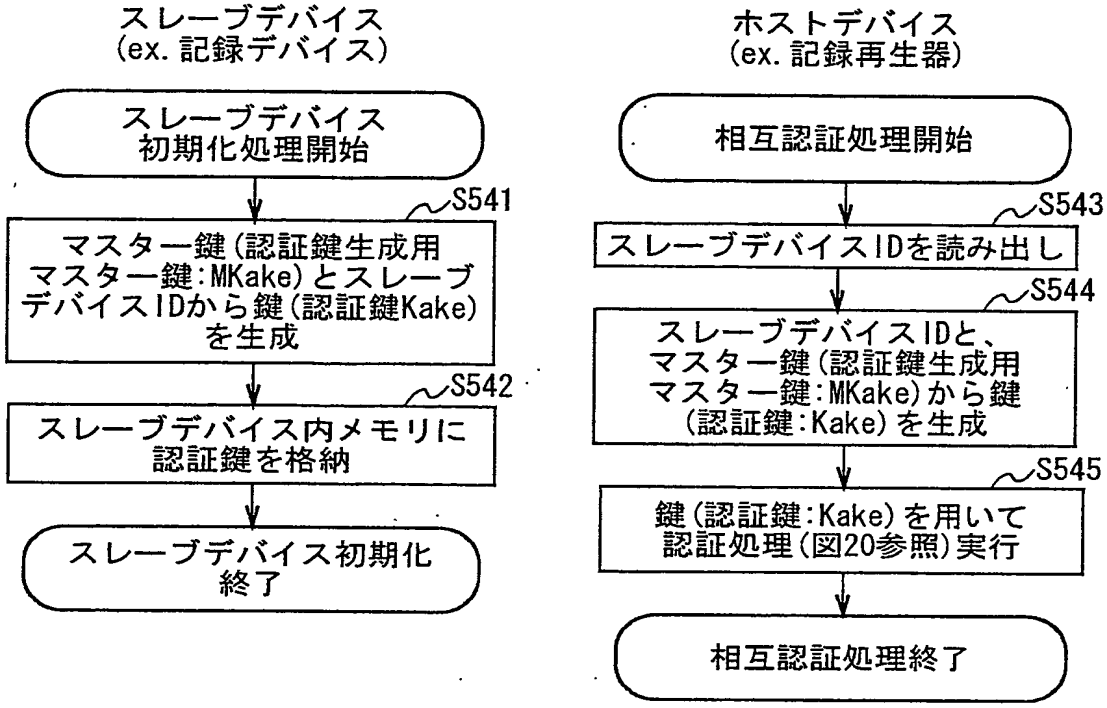


図５４

Master鍵から個別の鍵を生成する方法-(5)

[基本フロー]



[鍵所有構成]

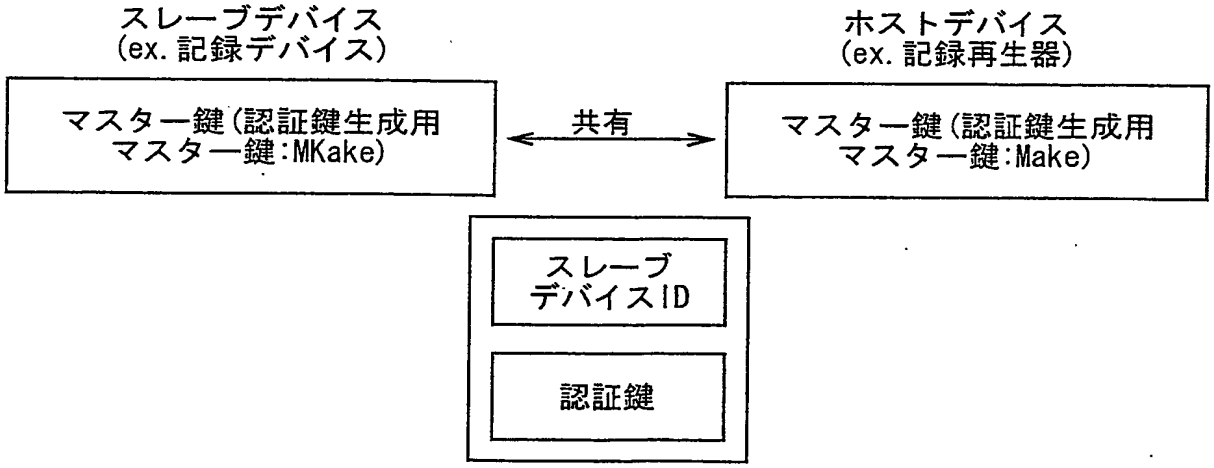


図５５

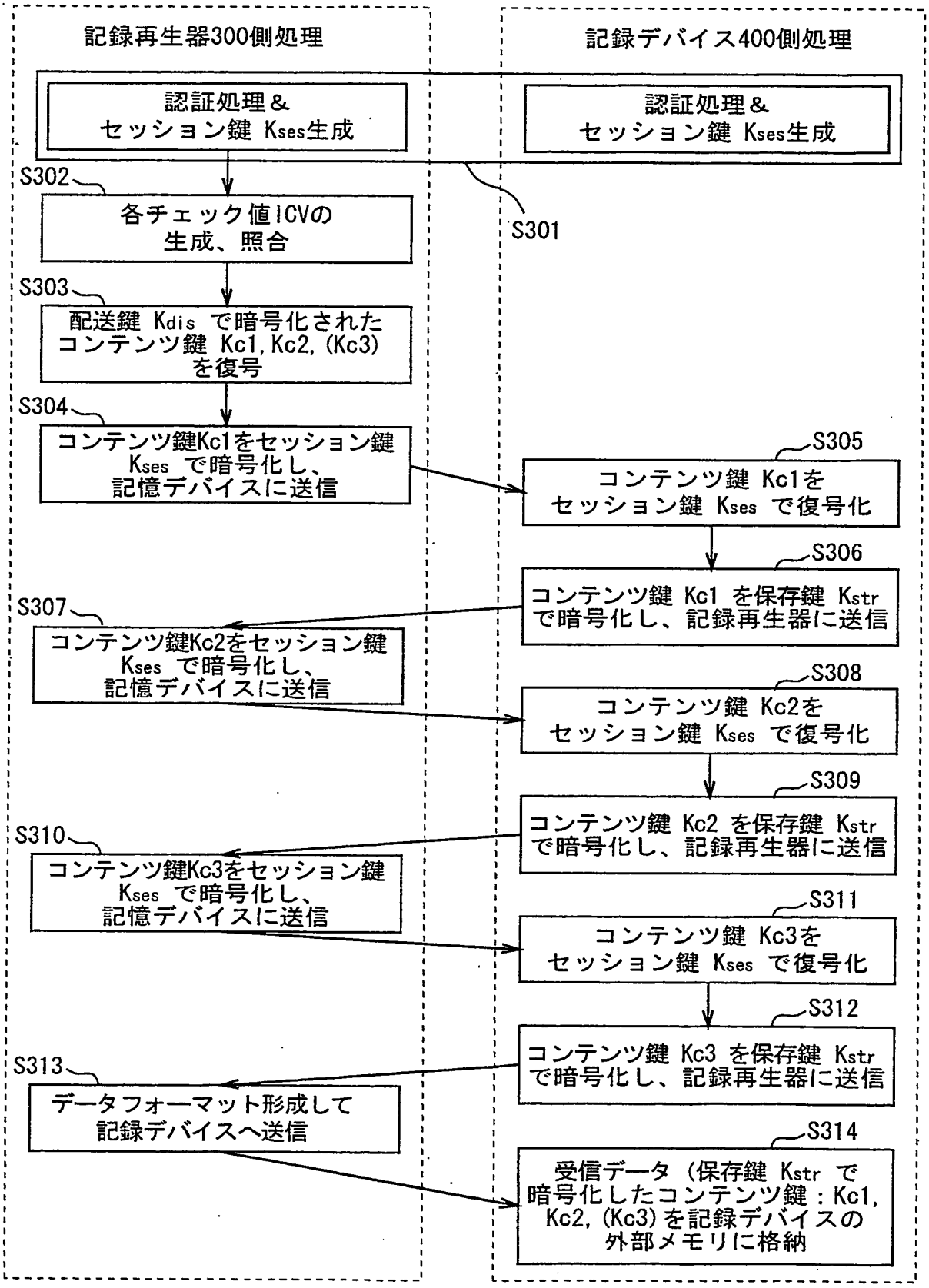

トリプルＤＥＳコンテンツ鍵：Kc1, Kc2, (Kc3)の格納（ダウンロード）処理
記録再生器300側処理
記録デバイス400側処理
認証処理＆
セッション鍵 Kses生成
認証処理＆
セッション鍵 Kses生成
S301
S302
各チェック値ICVの
生成、照合
S303
配送鍵 Kdis で暗号化された
コンテンツ鍵 Kc1, Kc2, (Kc3)
を復号
S304
コンテンツ鍵Kc1をセッション鍵
Kses で暗号化し、
記憶デバイスに送信
S305
コンテンツ鍵 Kc1を
セッション鍵 Kses で復号化
S306
コンテンツ鍵 Kc1 を保存鍵 Kstr
で暗号化し、記録再生器に送信
S307
コンテンツ鍵Kc2をセッション鍵
Kses で暗号化し、
記憶デバイスに送信
S308
コンテンツ鍵 Kc2を
セッション鍵 Kses で復号化
S309
コンテンツ鍵 Kc2 を保存鍵 Kstr
で暗号化し、記録再生器に送信
S310
コンテンツ鍵Kc3をセッション鍵
Kses で暗号化し、
記憶デバイスに送信
S311
コンテンツ鍵 Kc3を
セッション鍵 Kses で復号化
S312
コンテンツ鍵 Kc3 を保存鍵 Kstr
で暗号化し、記録再生器に送信
S313
データフォーマット形成して
記録デバイスへ送信
S314
受信データ（保存鍵 Kstr で
暗号化したコンテンツ鍵：Kc1,
Kc2, (Kc3)を記録デバイスの
外部メモリに格納

図５６

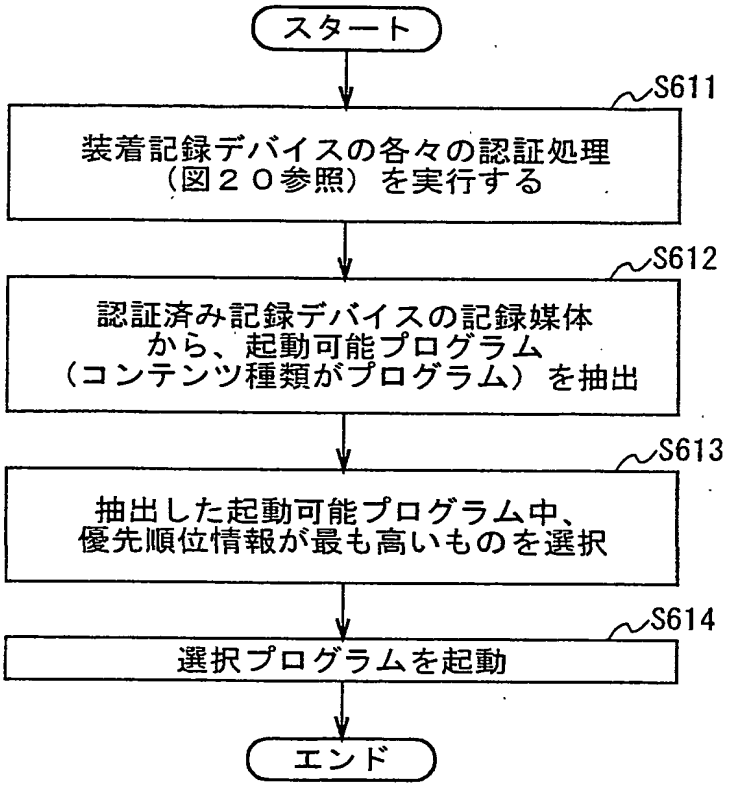

スタート
S611
装着記録デバイスの各々の認証処理
（図２０参照）を実行する
S612
認証済み記録デバイスの記録媒体
から、起動可能プログラム
（コンテンツ種類がプログラム）を抽出
S613
抽出した起動可能プログラム中、
優先順位情報が最も高いものを選択
S614
選択プログラムを起動
エンド

図５７

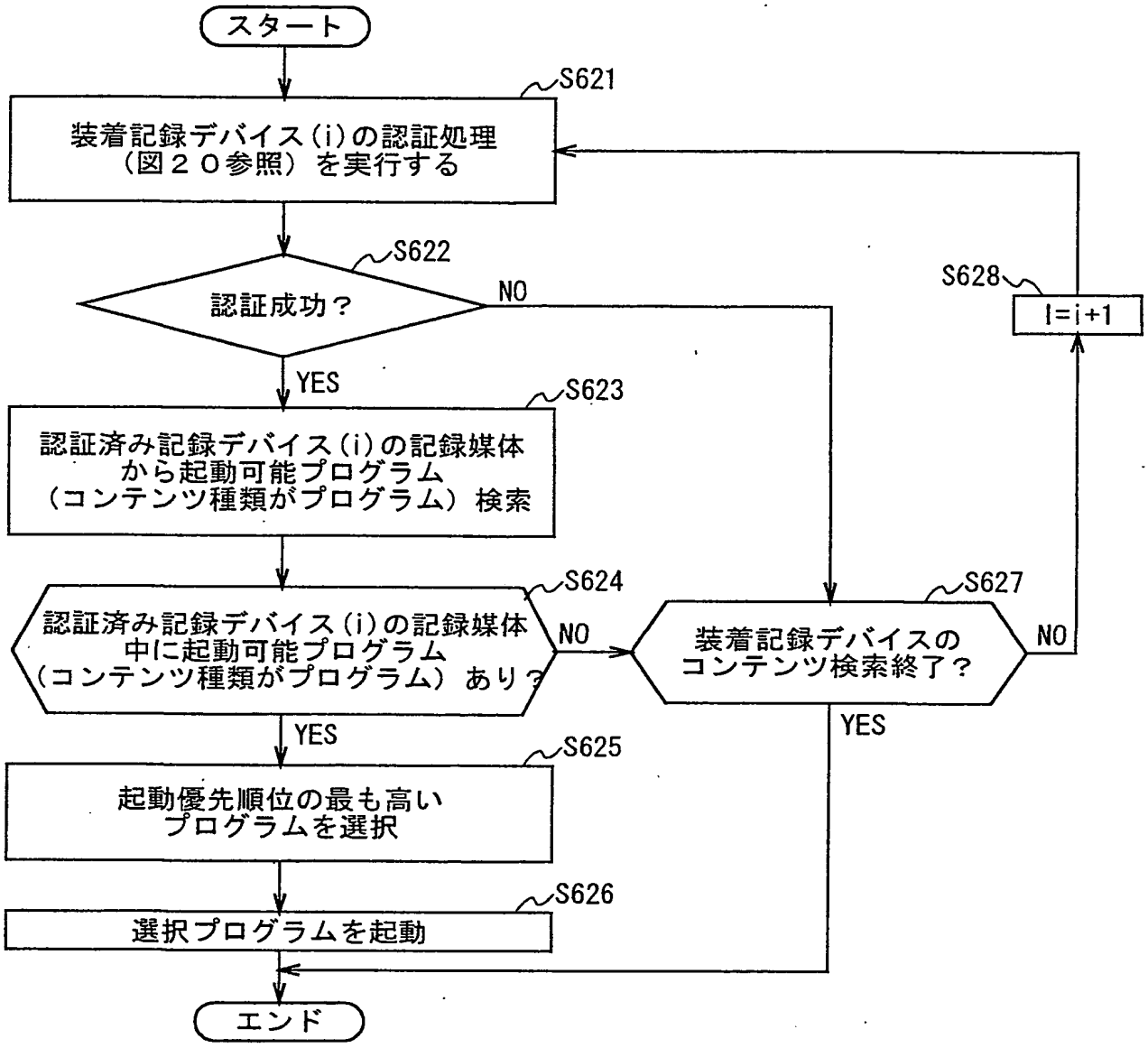

スタート
S621
装着記録デバイス(i)の認証処理
（図２０参照）を実行する
S622
認証成功？
NO
YES
S623
認証済み記録デバイス(i)の記録媒体
から起動可能プログラム
（コンテンツ種類がプログラム）検索
S624
認証済み記録デバイス(i)の記録媒体
中に起動可能プログラム
（コンテンツ種類がプログラム）あり？
NO
YES
S625
起動優先順位の最も高い
プログラムを選択
S626
選択プログラムを起動
エンド
S627
装着記録デバイスの
コンテンツ検索終了？
NO
YES
S628
I=i+1

図５８

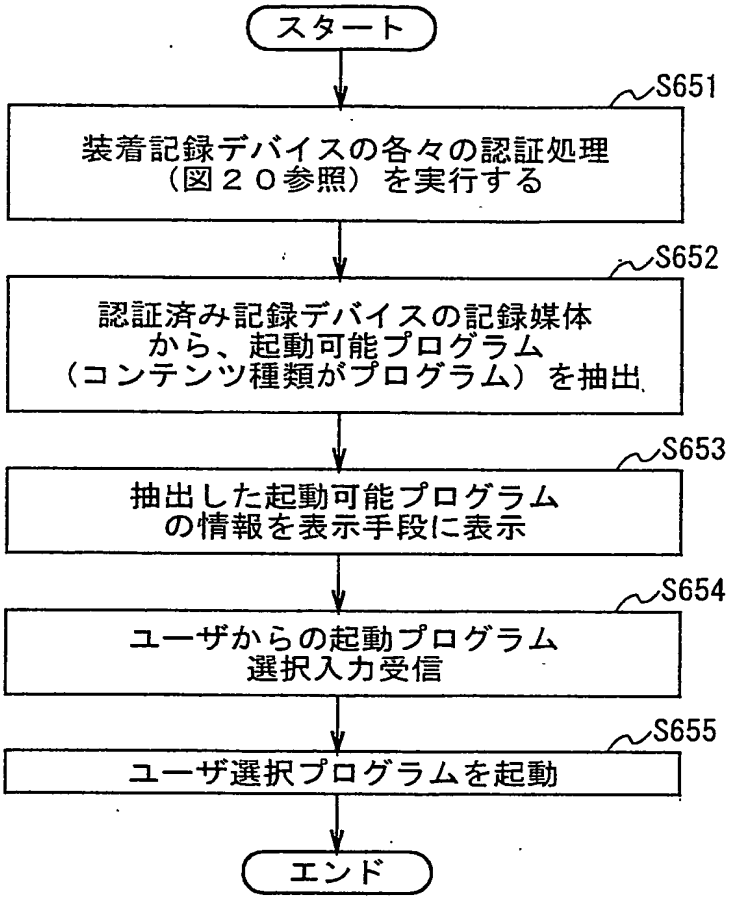

スタート
S651
装着記録デバイスの各々の認証処理
（図２０参照）を実行する
S652
認証済み記録デバイスの記録媒体
から、起動可能プログラム
（コンテンツ種類がプログラム）を抽出
S653
抽出した起動可能プログラム
の情報を表示手段に表示
S654
ユーザからの起動プログラム
選択入力受信
S655
ユーザ選択プログラムを起動
エンド

図５９

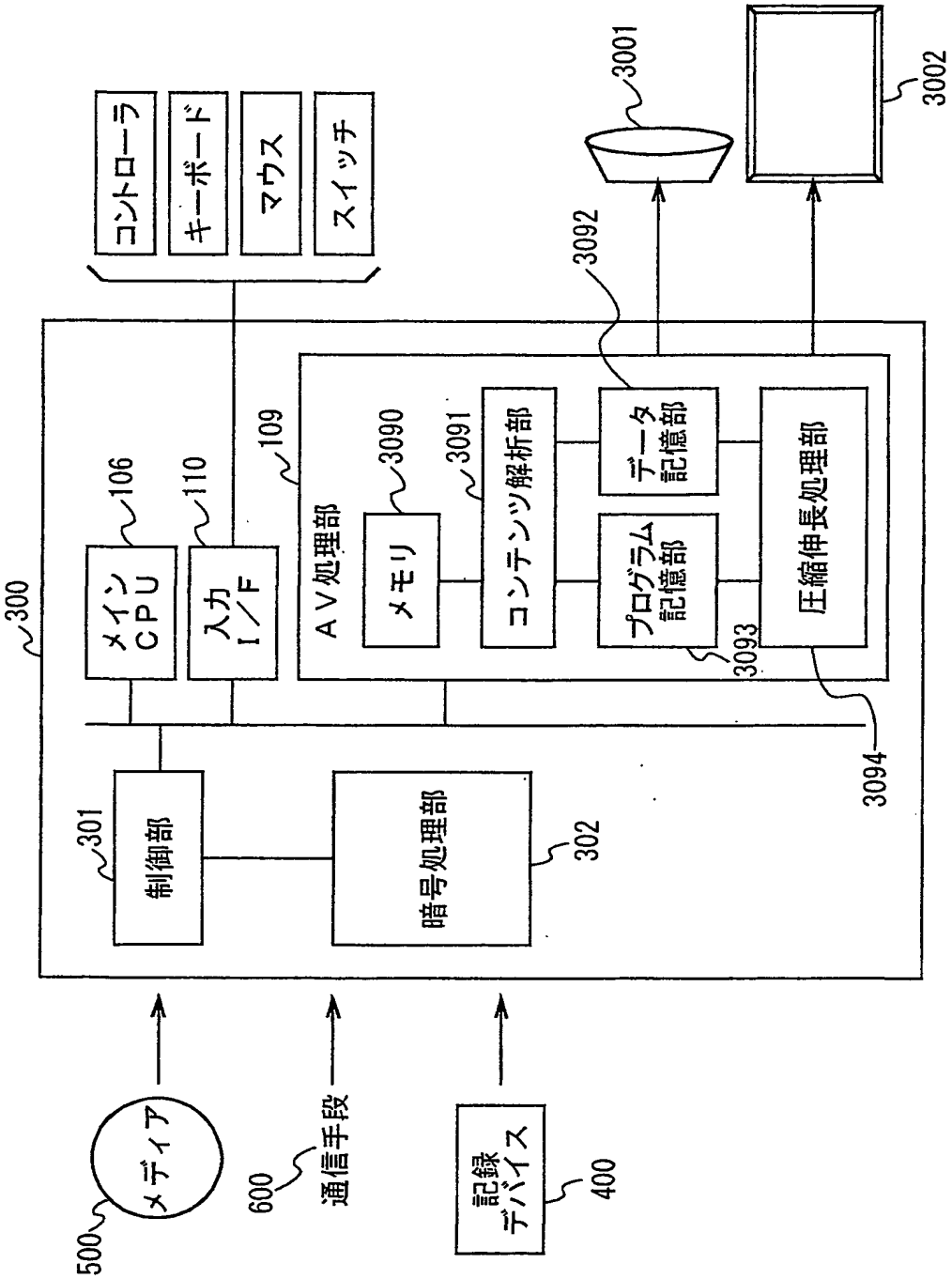

コントローラ
キーボード
マウス
スイッチ
3001
3002
3092
300
メイン CPU
106
入力 I／F
110
109
AV処理部
3090
メモリ
3091
コンテンツ解析部
データ記憶部
プログラム記憶部
3093
圧縮伸長処理部
3094
301
制御部
暗号処理部
302
メディア
500
600
通信手段
記録デバイス
400

図６０

コンテンツ構成例（１）

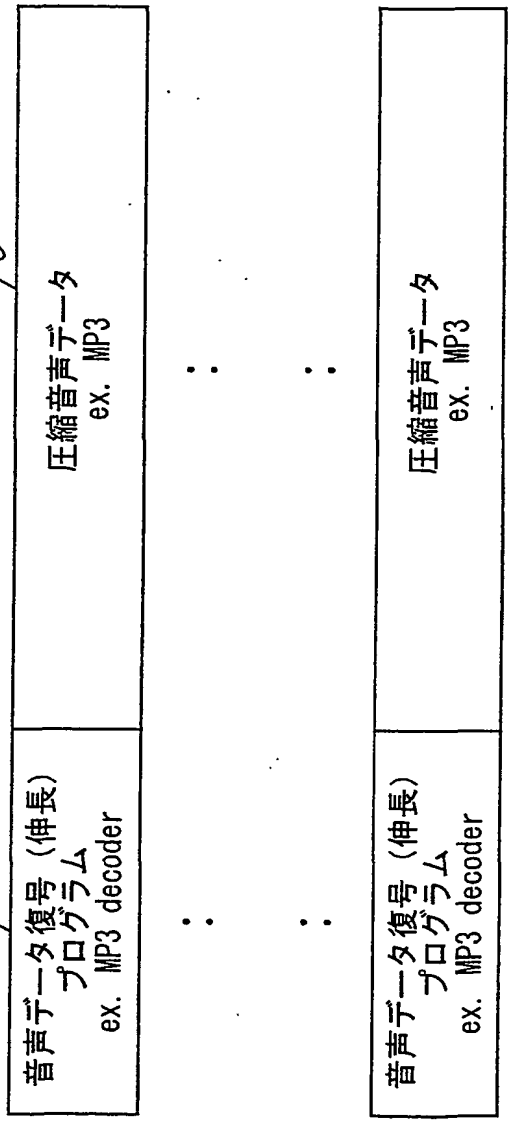


図６１

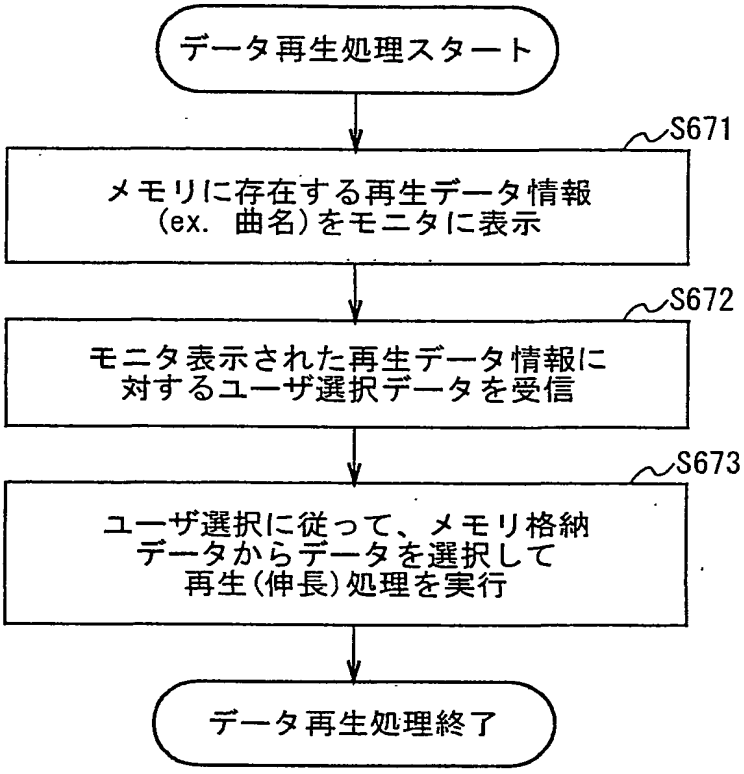

データ再生処理スタート
S671
メモリに存在する再生データ情報
(ex. 曲名)をモニタに表示
S672
モニタ表示された再生データ情報に
対するユーザ選択データを受信
S673
ユーザ選択に従って、メモリ格納
データからデータを選択して
再生(伸長)処理を実行
データ再生処理終了

図６２

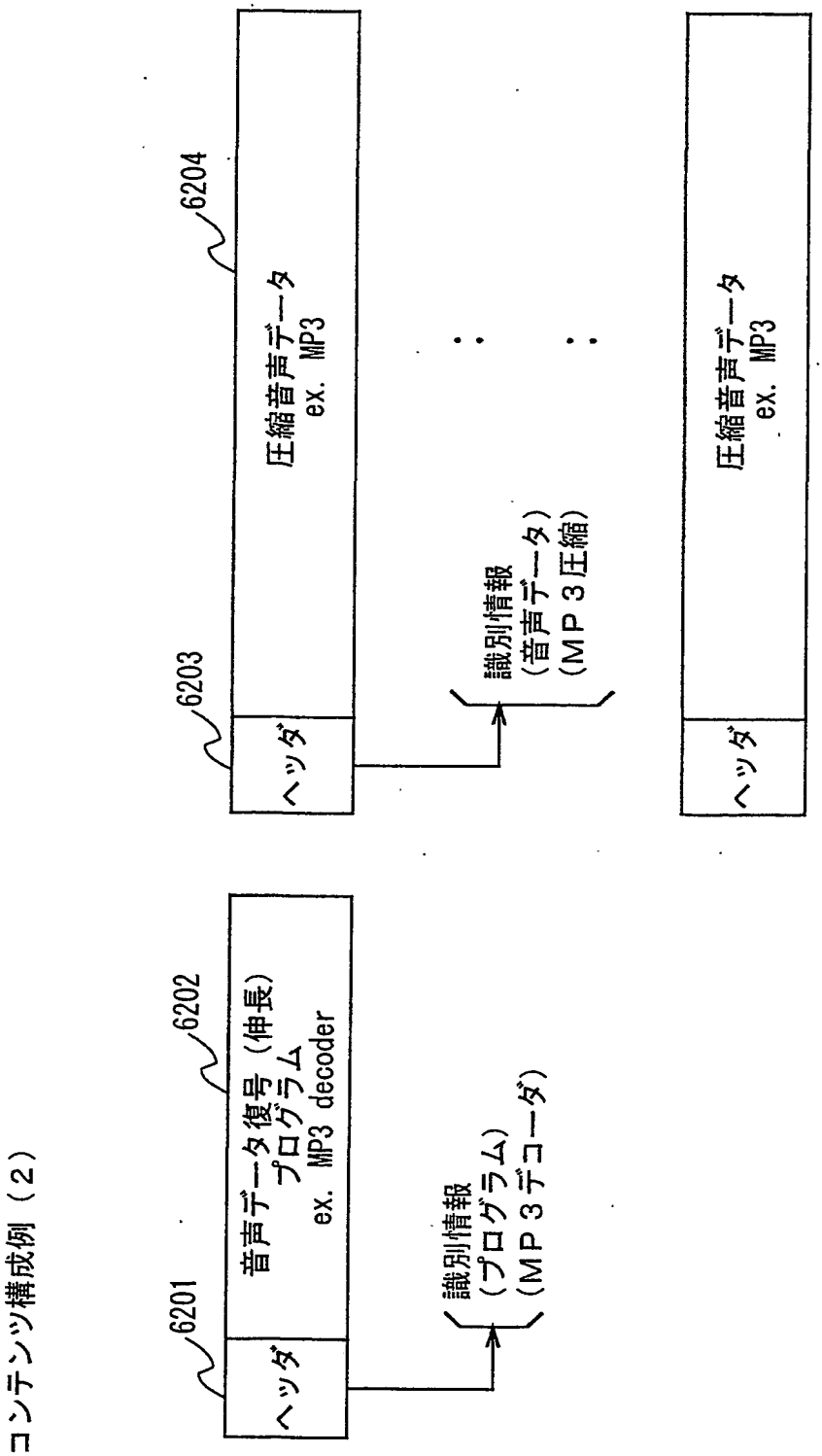

コンテンツ構成例（２）
6201
ヘッダ
6202
音声データ復号（伸長）
プログラム
ex. MP3 decoder
識別情報
（プログラム）
（ＭＰ３デコーダ）
6203
ヘッダ
6204
圧縮音声データ
ex. MP3
識別情報
（音声データ）
（ＭＰ３圧縮）
ヘッダ
圧縮音声データ
ex. MP3

図６３

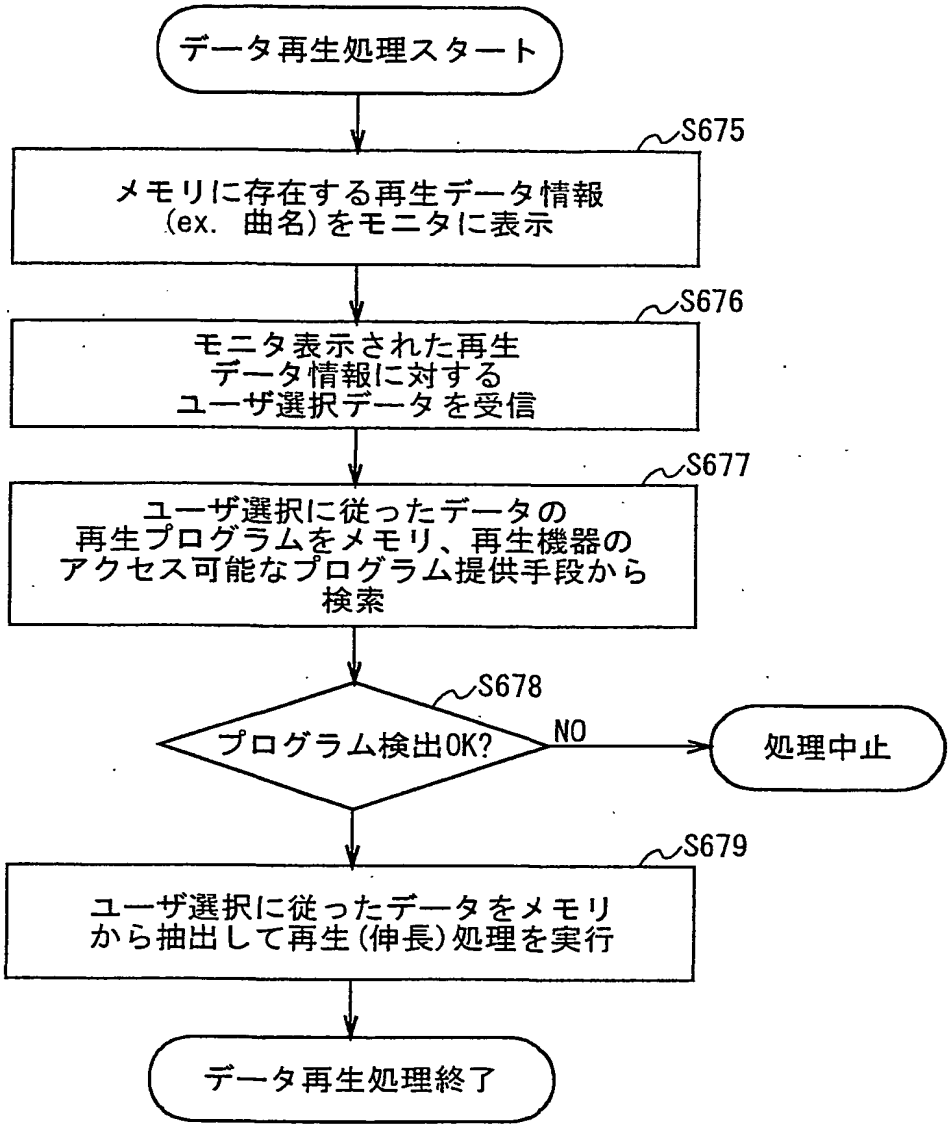

データ再生処理スタート
S675
メモリに存在する再生データ情報
(ex. 曲名)をモニタに表示
S676
モニタ表示された再生
データ情報に対する
ユーザ選択データを受信
S677
ユーザ選択に従ったデータの
再生プログラムをメモリ、再生機器の
アクセス可能なプログラム提供手段から
検索
S678
プログラム検出OK?
NO
処理中止
S679
ユーザ選択に従ったデータをメモリ
から抽出して再生(伸長)処理を実行
データ再生処理終了

図６４

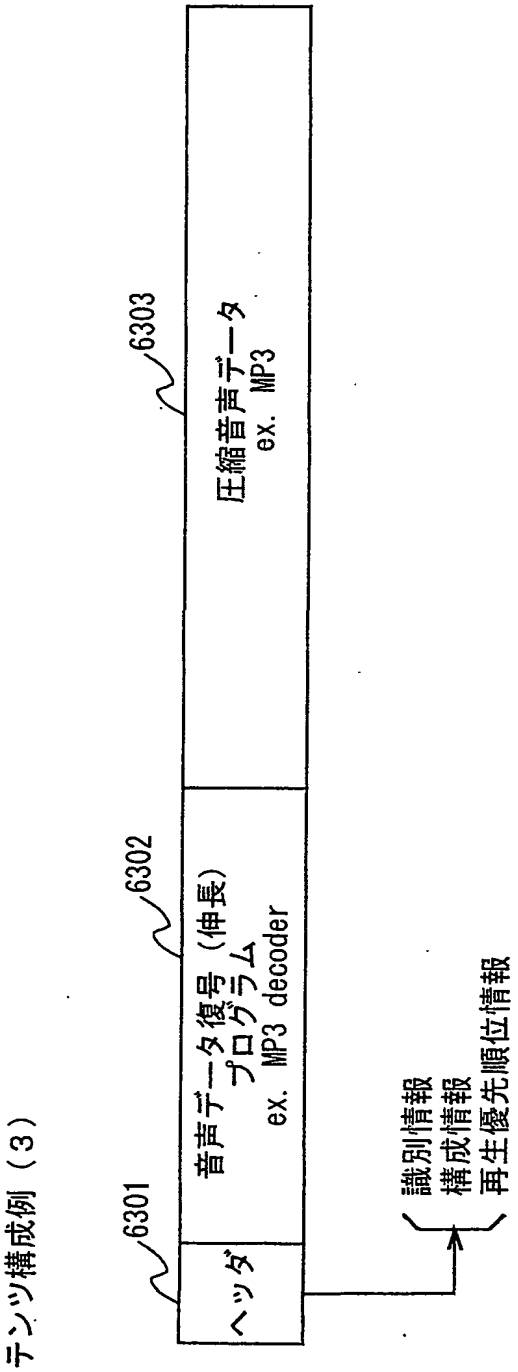

コンテンツ構成例（３）
6301
ヘッダ
6302
音声データ復号（伸長）プログラム
ex. MP3 decoder
6303
圧縮音声データ
ex. MP3
識別情報
構成情報
再生優先順位情報

図６５

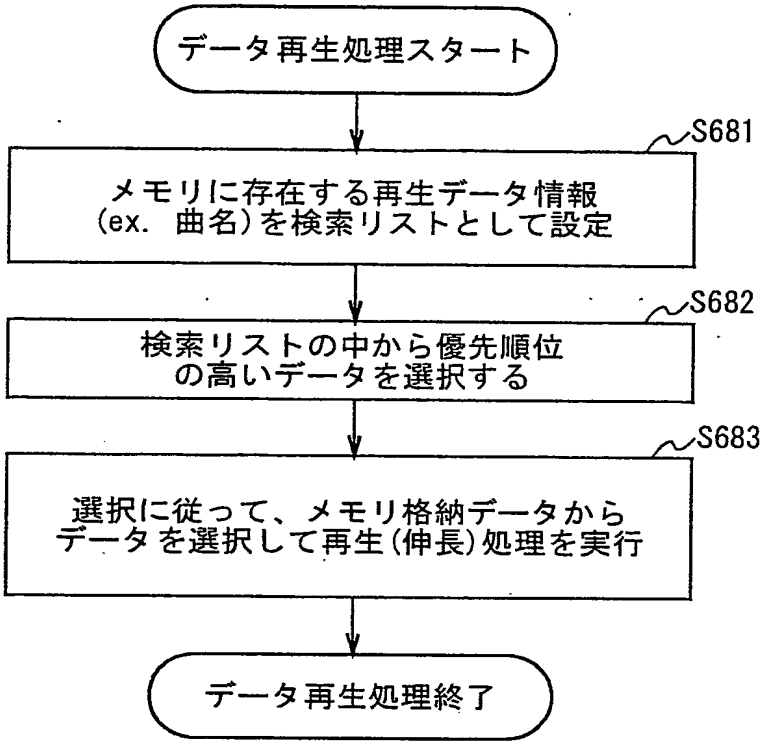

データ再生処理スタート
S681
メモリに存在する再生データ情報
(ex. 曲名)を検索リストとして設定
S682
検索リストの中から優先順位
の高いデータを選択する
S683
選択に従って、メモリ格納データから
データを選択して再生(伸長)処理を実行
データ再生処理終了

図６６

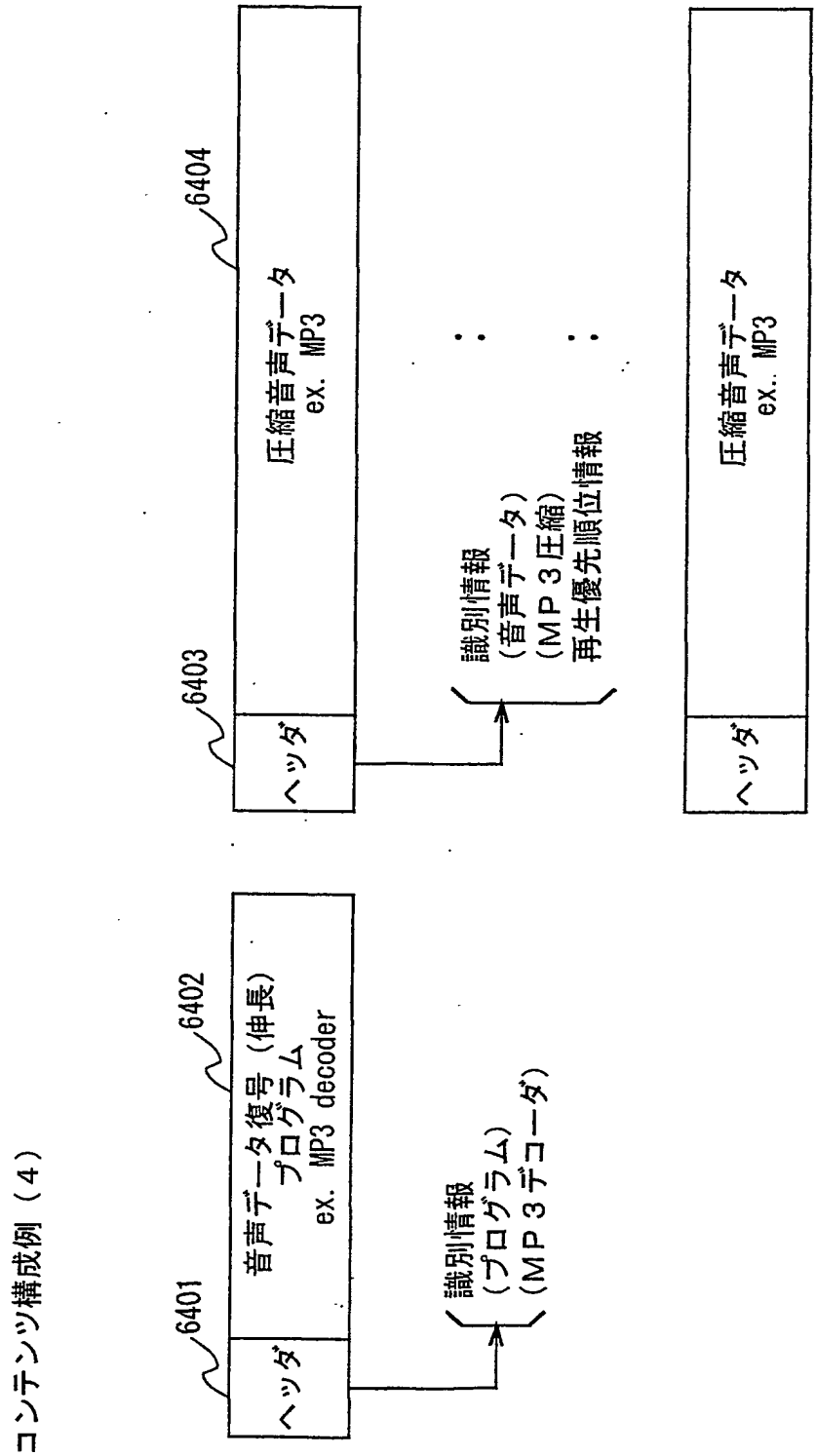

コンテンツ構成例（４）
6401
ヘッダ
音声データ復号（伸長）プログラム
ex. MP3 decoder
6402
識別情報
（プログラム）
（ＭＰ３デコーダ）
6403
ヘッダ
圧縮音声データ
ex. MP3
6404
識別情報
（音声データ）
（ＭＰ３圧縮）
再生優先順位情報
ヘッダ
圧縮音声データ
ex.. MP3

図６７

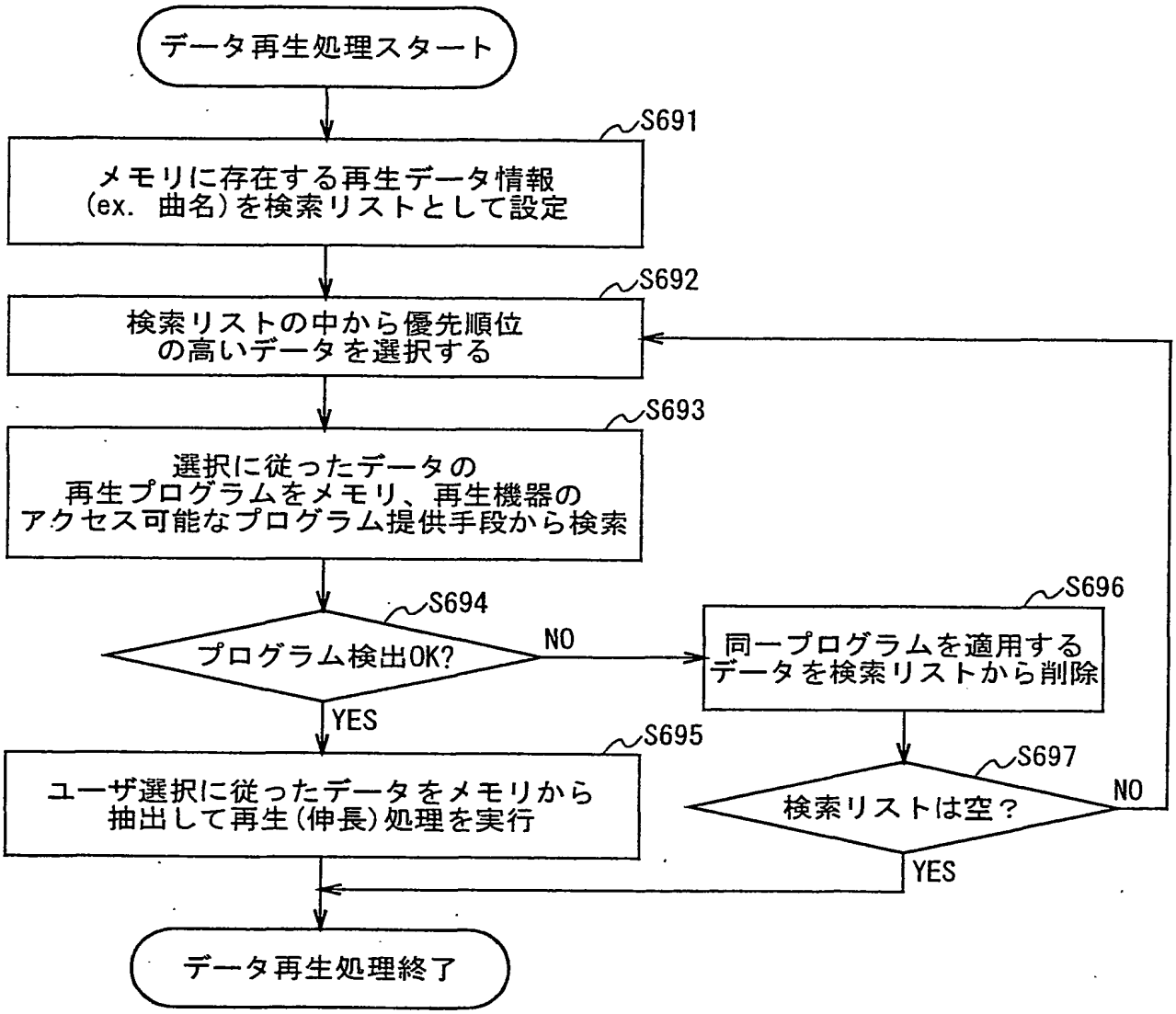

データ再生処理スタート
S691
メモリに存在する再生データ情報
(ex. 曲名)を検索リストとして設定
S692
検索リストの中から優先順位
の高いデータを選択する
S693
選択に従ったデータの
再生プログラムをメモリ、再生機器の
アクセス可能なプログラム提供手段から検索
S694
プログラム検出OK?
NO
S696
同一プログラムを適用する
データを検索リストから削除
YES
S695
ユーザ選択に従ったデータをメモリから
抽出して再生(伸長)処理を実行
S697
検索リストは空?
NO
YES
データ再生処理終了

図６８

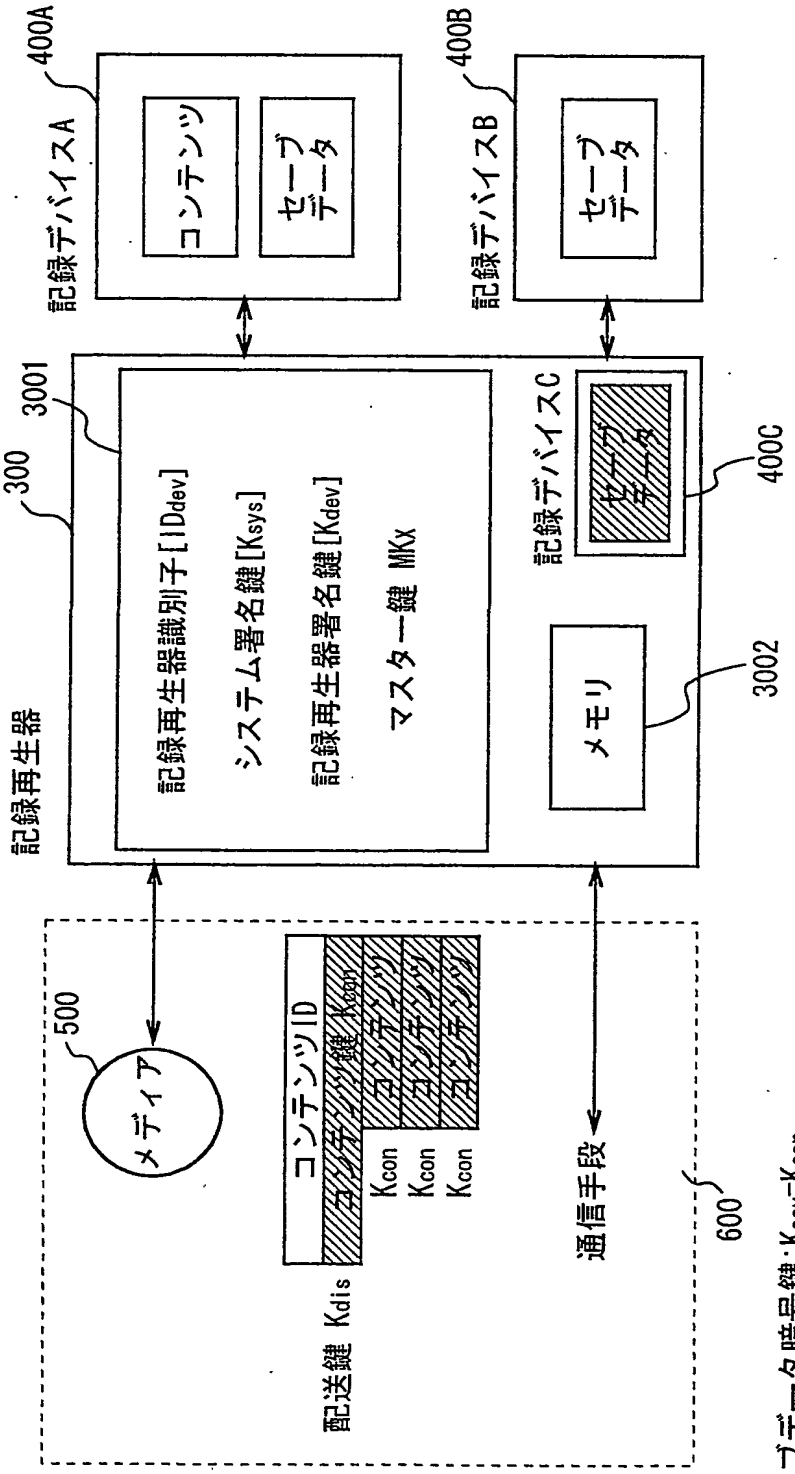

記録再生器
300
3001
記録再生器識別子[IDdev]
システム署名鍵[Ksys]
記録再生器署名鍵[Kdev]
マスター鍵 MKx
メモリ
3002
記録デバイスC
セーブデータ
400C
記録デバイスA
400A
コンテンツ
セーブデータ
記録デバイスB
400B
セーブデータ
メディア
500
コンテンツID
コンテンツ鍵 Kcon
コンテンツ
コンテンツ
コンテンツ
Kcon
Kcon
Kcon
配送鍵 Kdis
通信手段
600
セーブデータ暗号鍵:Ksav=Kcon
セーブデータ暗号鍵:Ksav=Ksys
セーブデータ暗号鍵:Ksav=Kdev
セーブデータ暗号鍵:Ksav=コンテンツID OR DES (MKx, コンテンツID)
セーブデータ暗号鍵:Ksav=記録再生器ID(IDdev) or DES (MKx, 記録再生器ID(IDdev))
セーブデータ暗号鍵:Ksav=(Kcon^Kdev)or DES(MKx, Kcon^Kdev)
セーブデータ暗号鍵:Ksav=(コンテンツID^Kdev)or DES(MKx, コンテンツID^Kdev)
セーブデータ暗号鍵:Ksav=(KCON^記録再生器ID) OR DES (MKx, KCON^記録再生器ID)
セーブデータ暗号鍵:Ksav=(コンテンツID^記録再生器ID) OR DES (MKX, コンテンツID^記録再生器ID)
セーブデータ暗号鍵:Ksav=パスワード OR DES(MKX, パスワード) 等

図69

(1) コンテンツ固有鍵、or システム共通鍵を使用したセーブデータ格納処理例

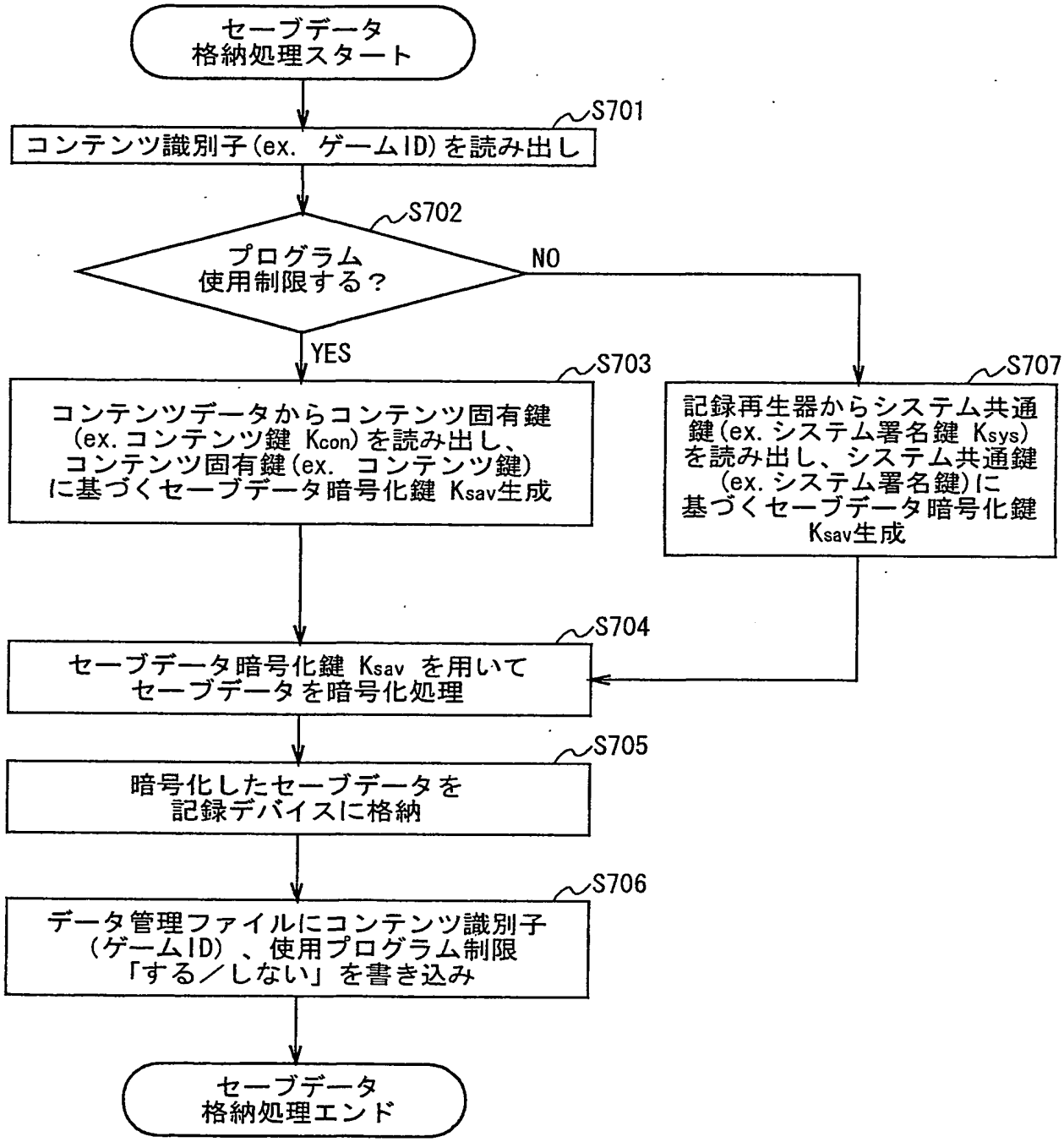


図７０

データ管理ファイル（１）

データ番号	コンテンツ識別子（ゲームＩＤ）	記録再生器識別子（ＩＤdev）	プログラム使用制限
1	12345678...	56789012...	する
2	ABCDEF12...	09876543...	する
3	12245678...	58834762...	しない
:	:	:	:

図７１

(2) コンテンツ固有鍵、or システム共通鍵を使用したセーブデータ再生処理例

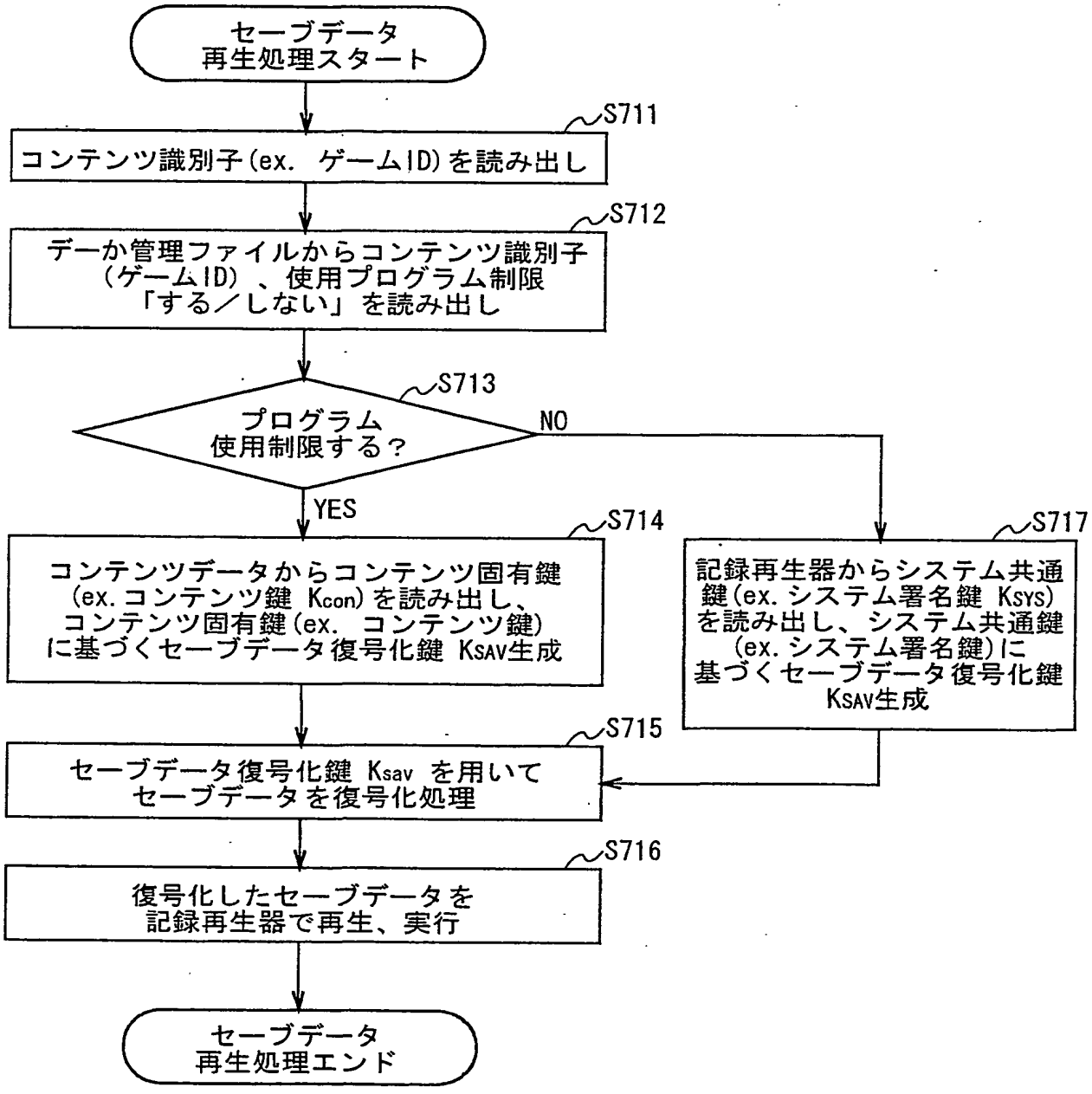


図７２

(3) コンテンツID、or システム共通鍵を使用したセーブデータ格納処理例

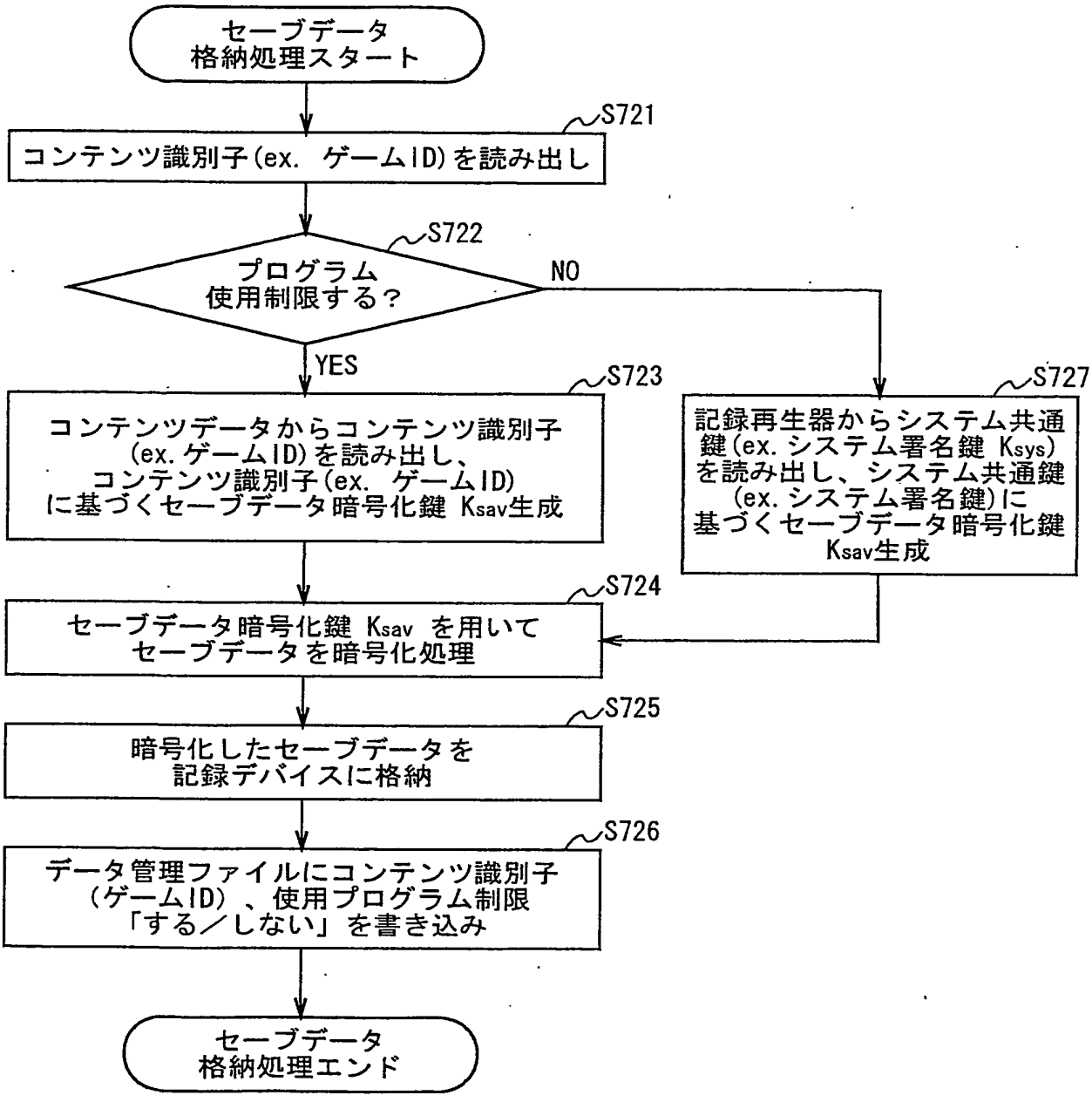


図７３

(4) コンテンツID、or システム共通鍵を使用したセーブデータ再生処理例

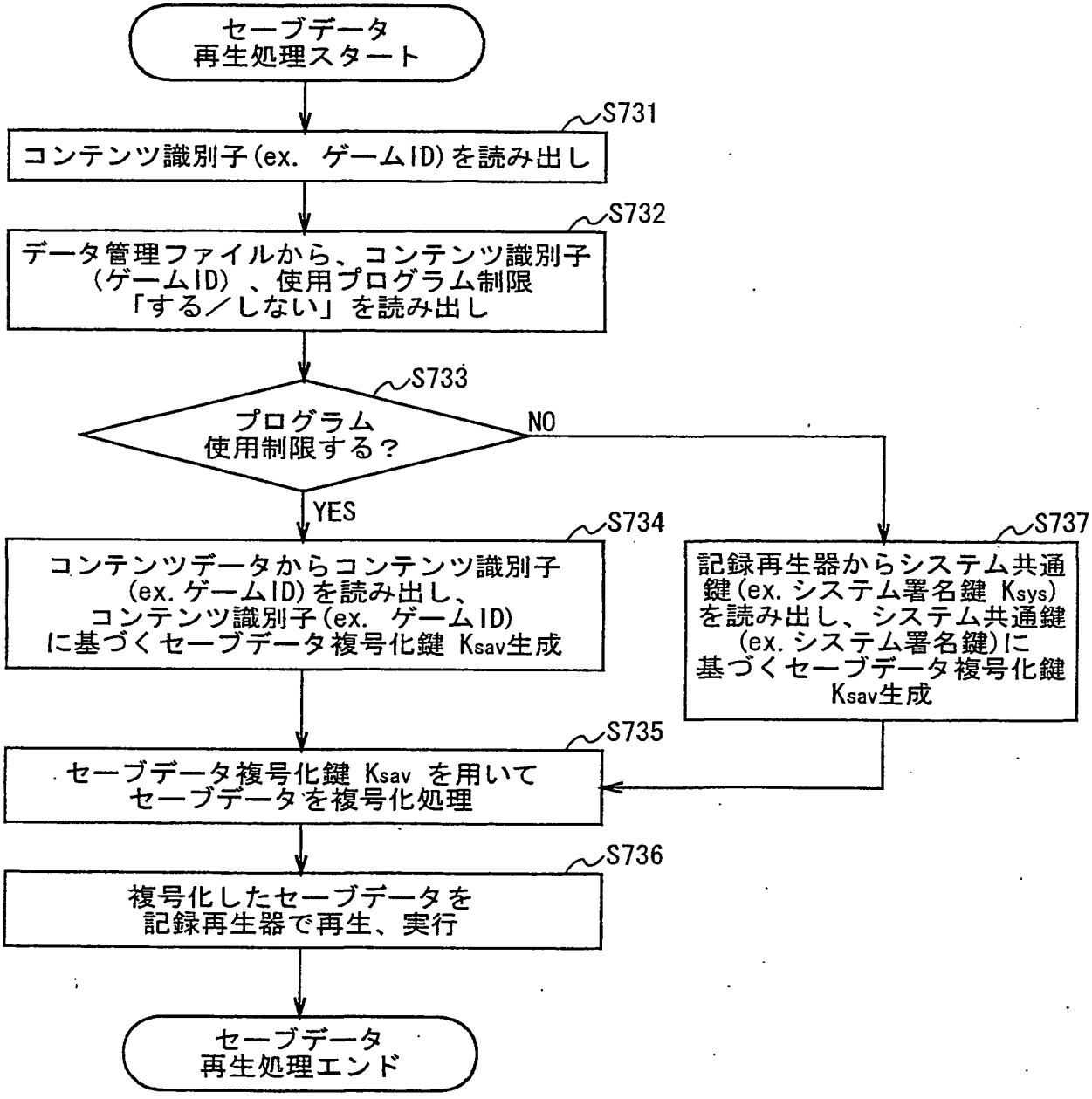


図７４

(5) 記録再生器固有鍵、or システム共通鍵を使用したセーブデータ格納処理例

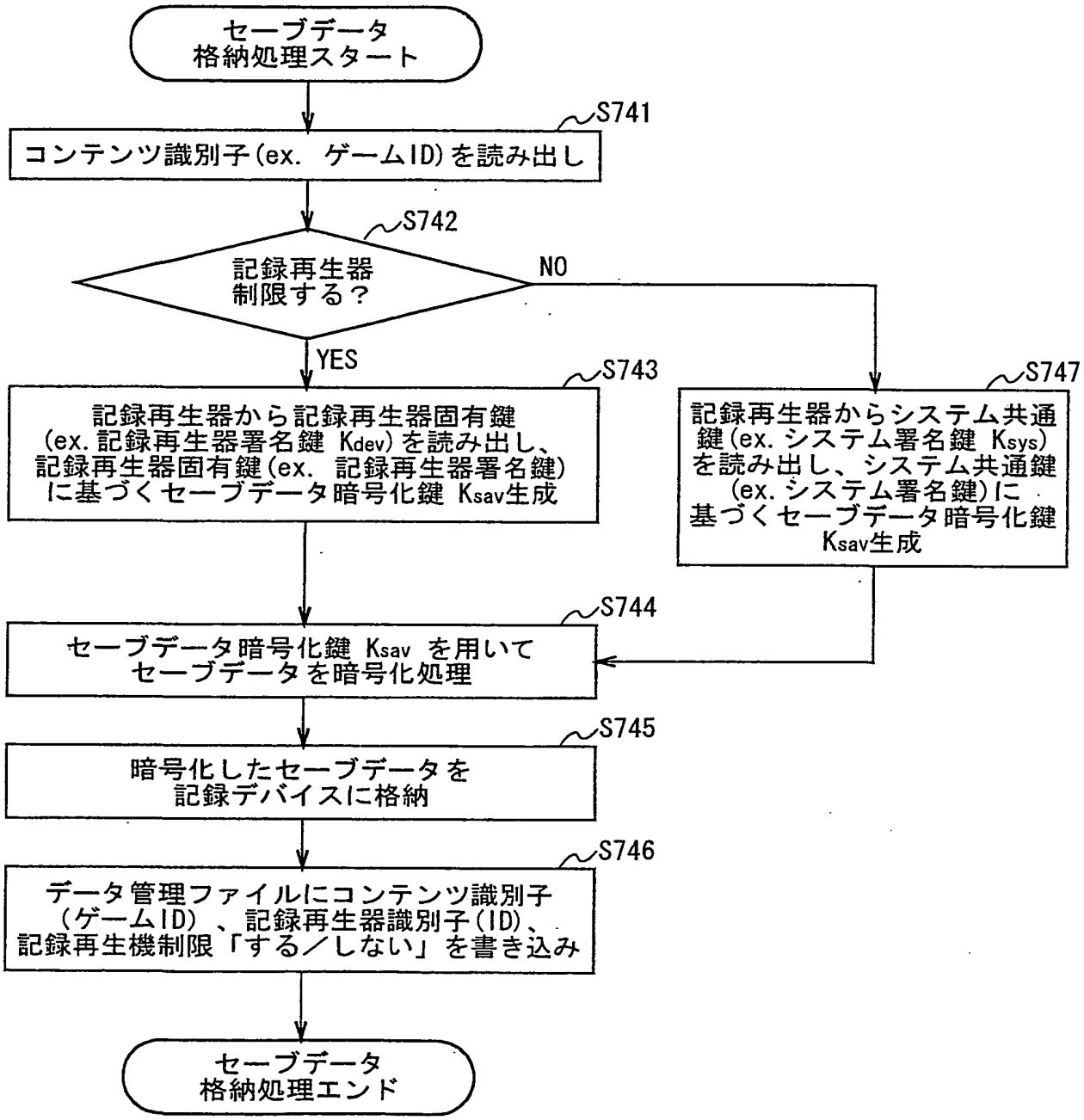


図７５

データ管理ファイル（２）

データ番号	コンテンツ識別子（ゲームＩＤ）	記録再生器識別子（ＩＤdev）	記録再生器制限
1	12345678...	56789012...	しない
2	ABCDEF12...	09876543...	する
3	12245678...	58834762...	する
:	:	:	:

図７６

(6) 記録再生器固有鍵、or システム共通鍵を使用したセーブデータ再生処理例

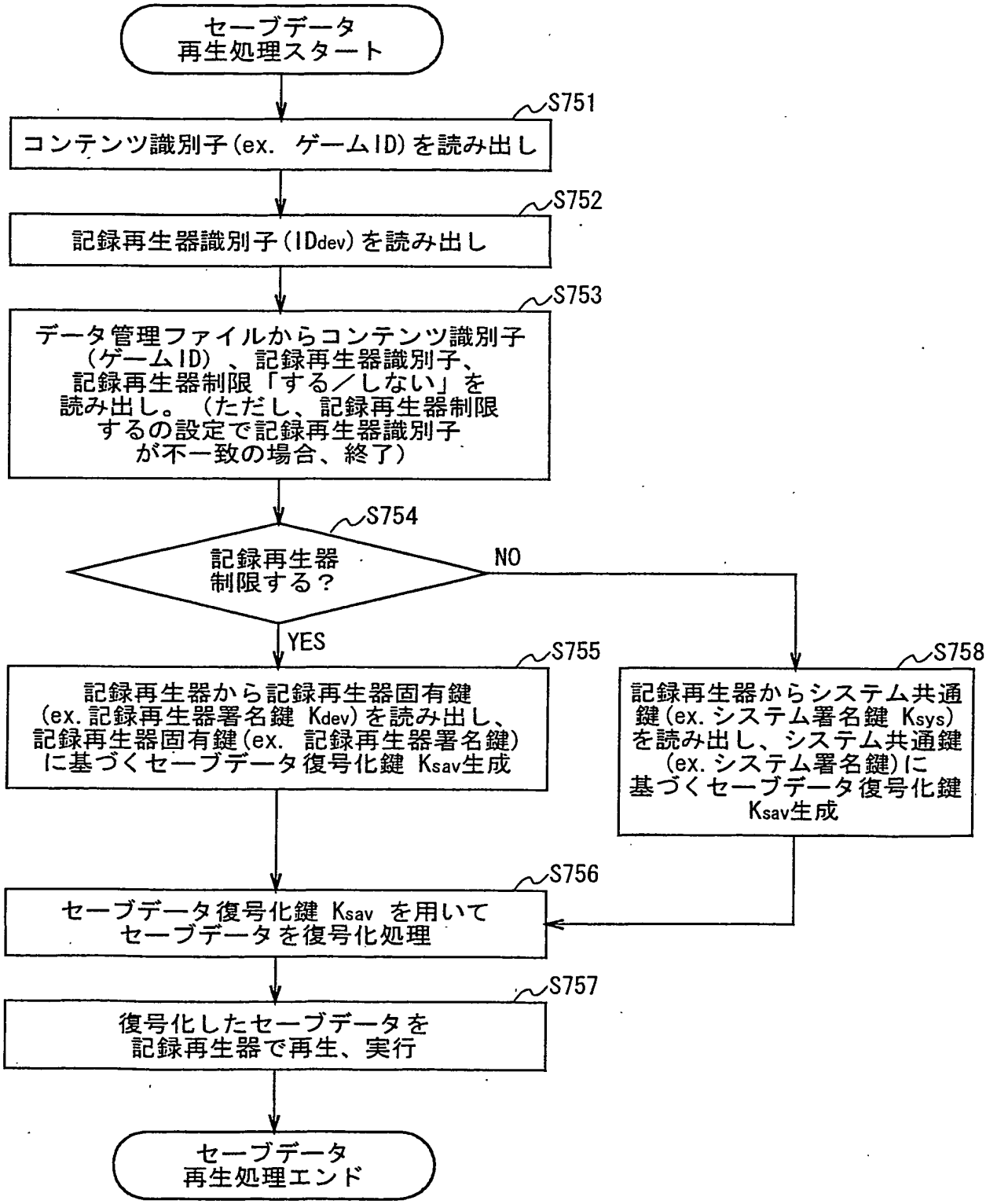


図７７

(7) 記録再生器識別子、or システム共通鍵を使用したセーブデータ格納処理例

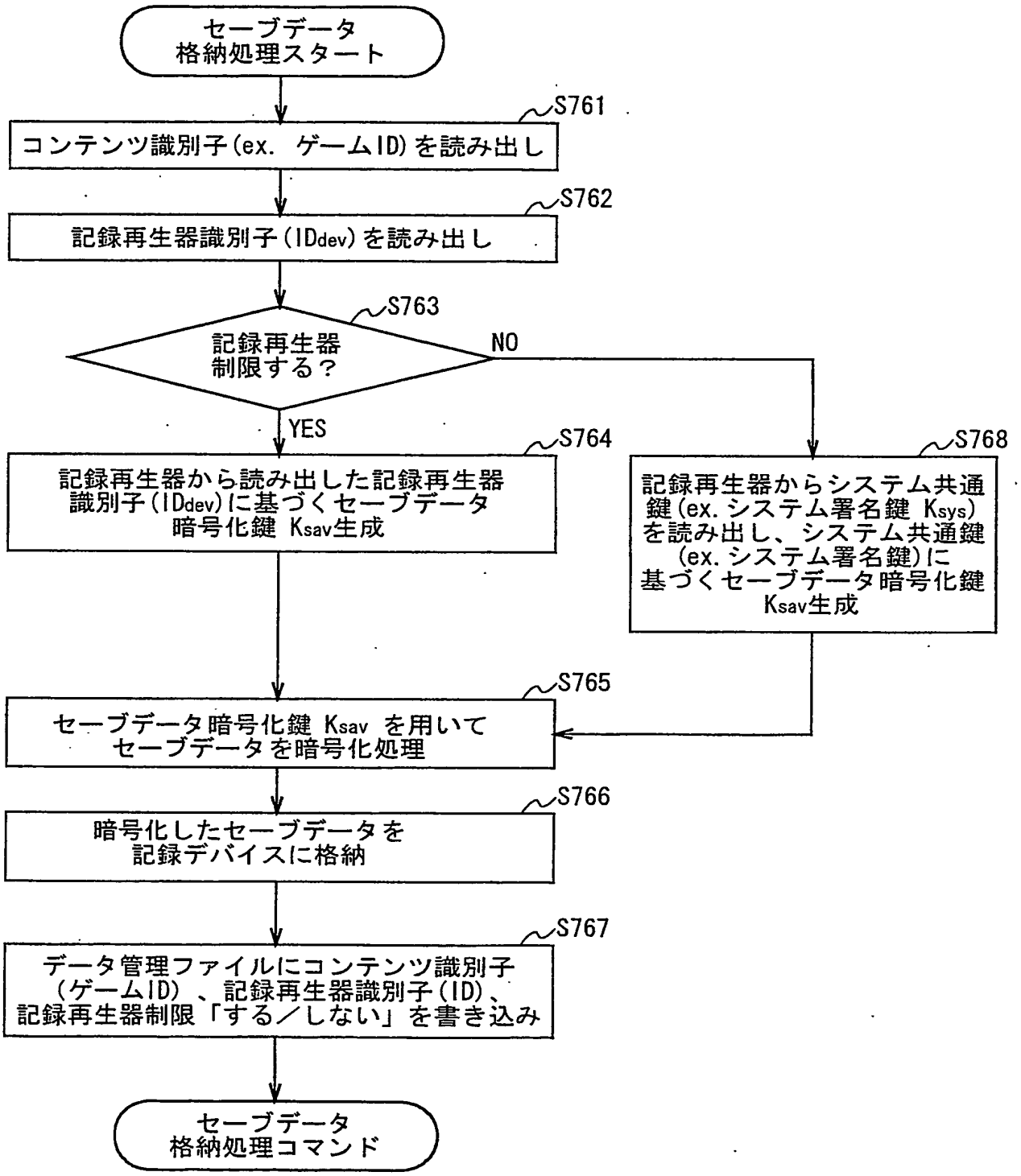


図７８

(8) 記録再生器識別子、or システム共通鍵を使用したセーブデータ再生処理例

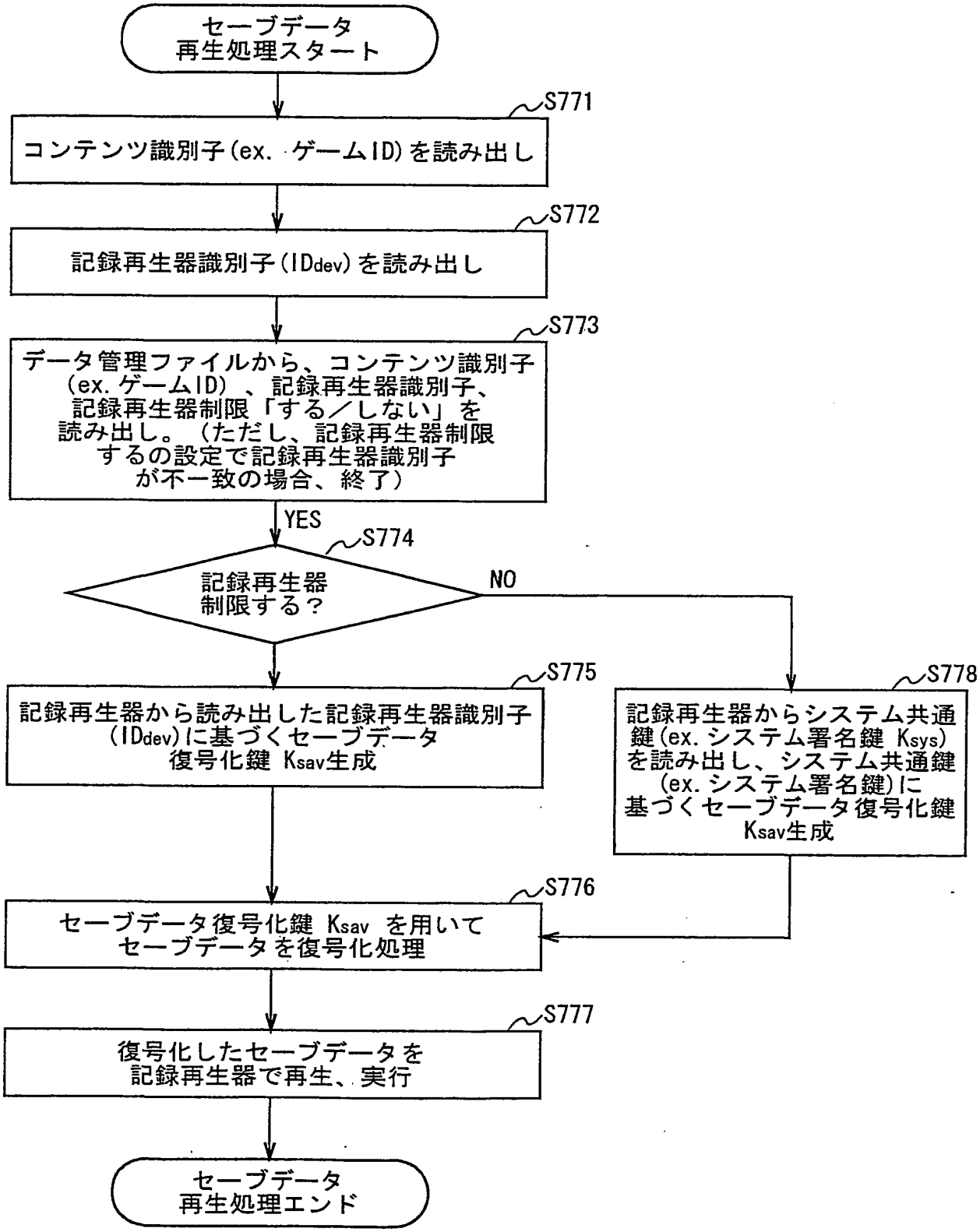


図７９

(9) コンテンツ固有鍵、記録再生器固有鍵、orシステム共通鍵を使用したセーブデータ格納処理例

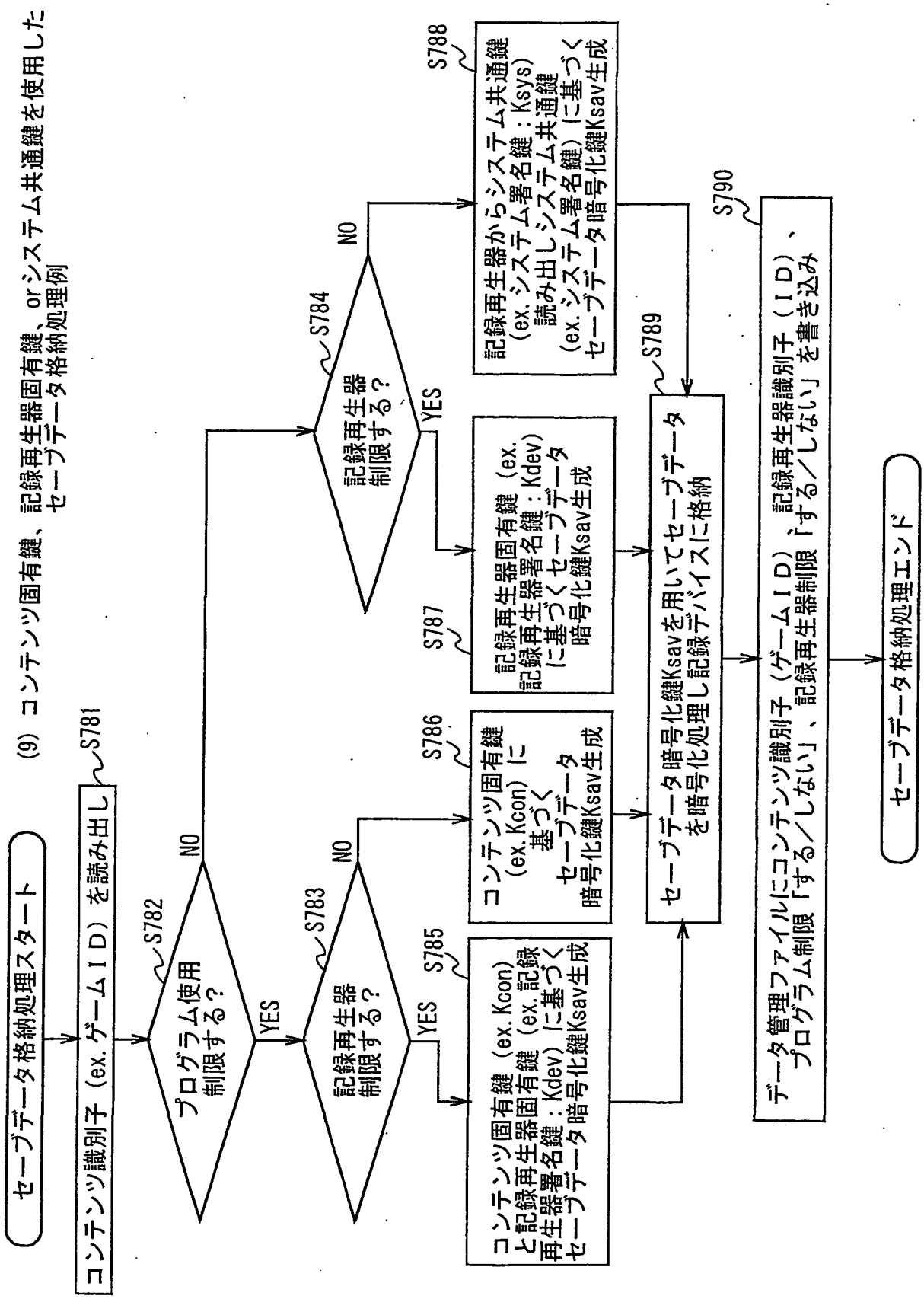


図８０

データ管理ファイル（３）

データ番号	コンテンツ識別子（ゲームＩＤ）	記録再生器識別子（ＩＤdev）	プログラム使用制限	記録再生器制限
1	12345678...	56789012...	する	しない
2	ABCDEF12...	09876543...	する	する
3	12245678...	58834762...	しない	する
:	:	:	:	:

図８１

(10) コンテンツ固有鍵、記録再生器固有鍵、
orシステム共通鍵を使用したセーブデータ再生処理例

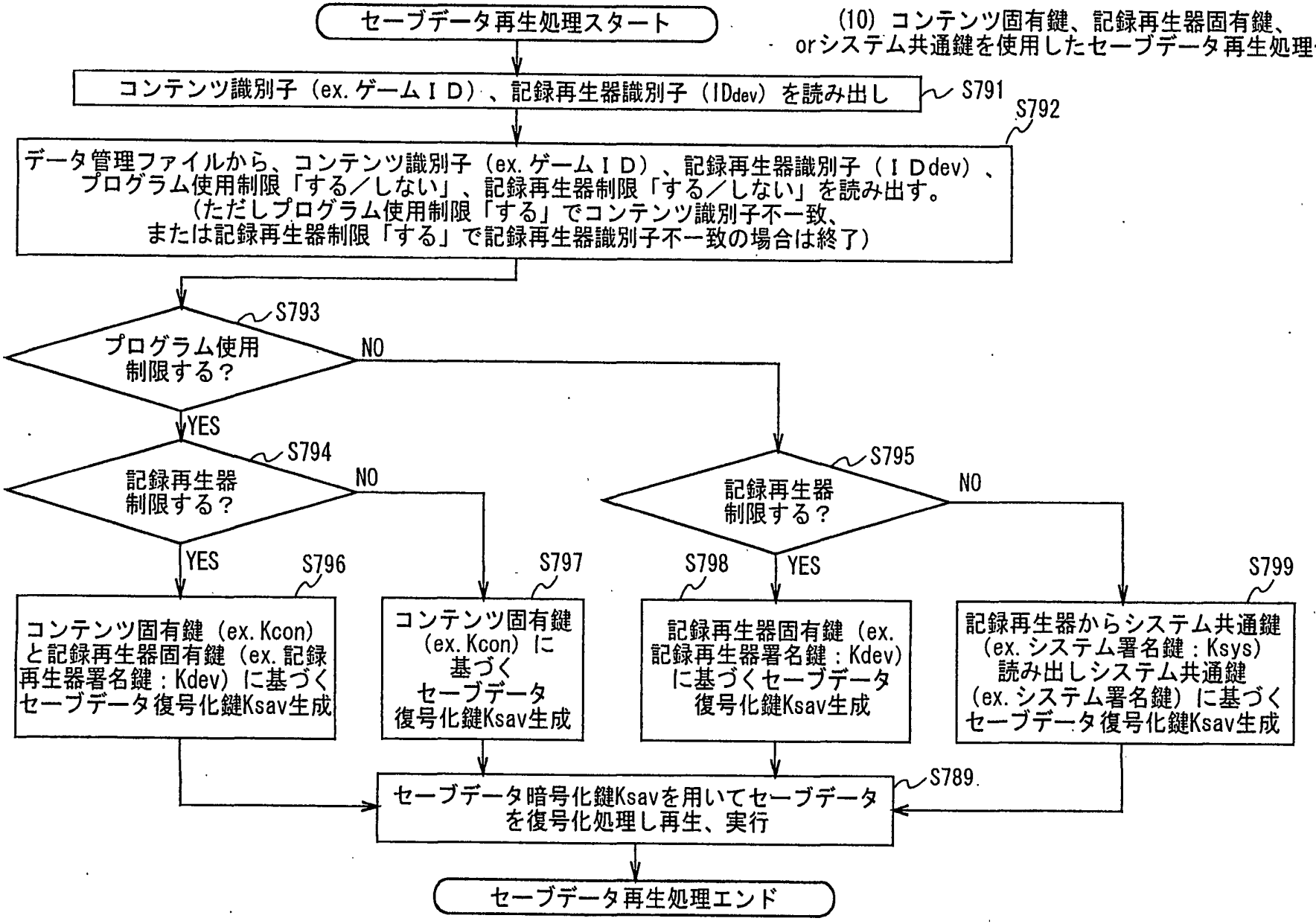


図８２

(11) ユーザパスワード、or システム共通鍵を使用したセーブデータ格納処理例

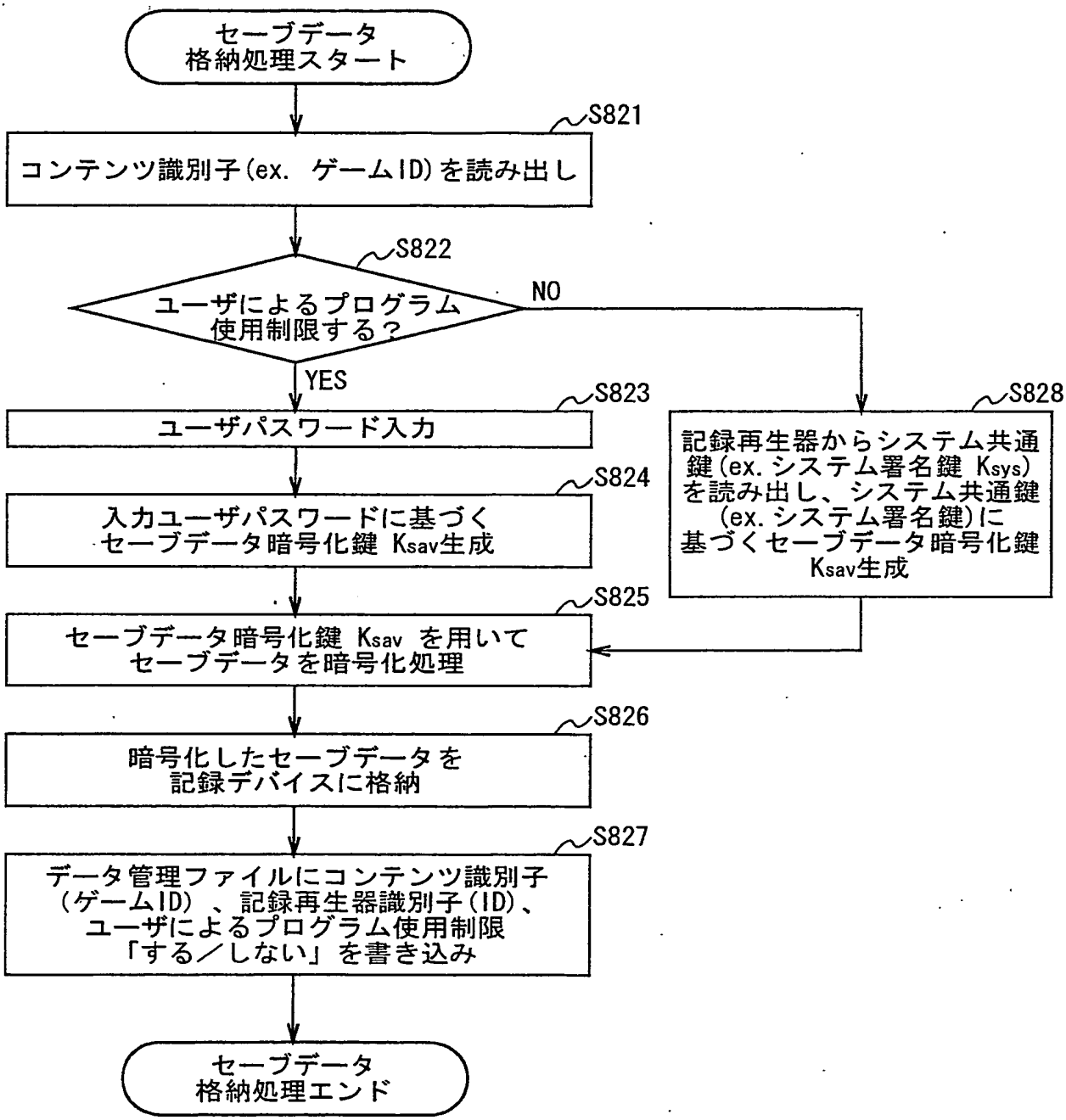


図８３

データ管理ファイル（４）

データ番号	コンテンツ識別子（ゲームＩＤ）	記録再生器識別子（ＩＤdev）	ユーザによるプログラム使用制限
1	12345678...	56789012...	する
2	ABCDEF12...	09876543...	する
3	12245678...	58834762...	しない
:	:	:	:

図８４

(12) ユーザパスワード、or システム共通鍵を使用したセーブデータ再生処理例

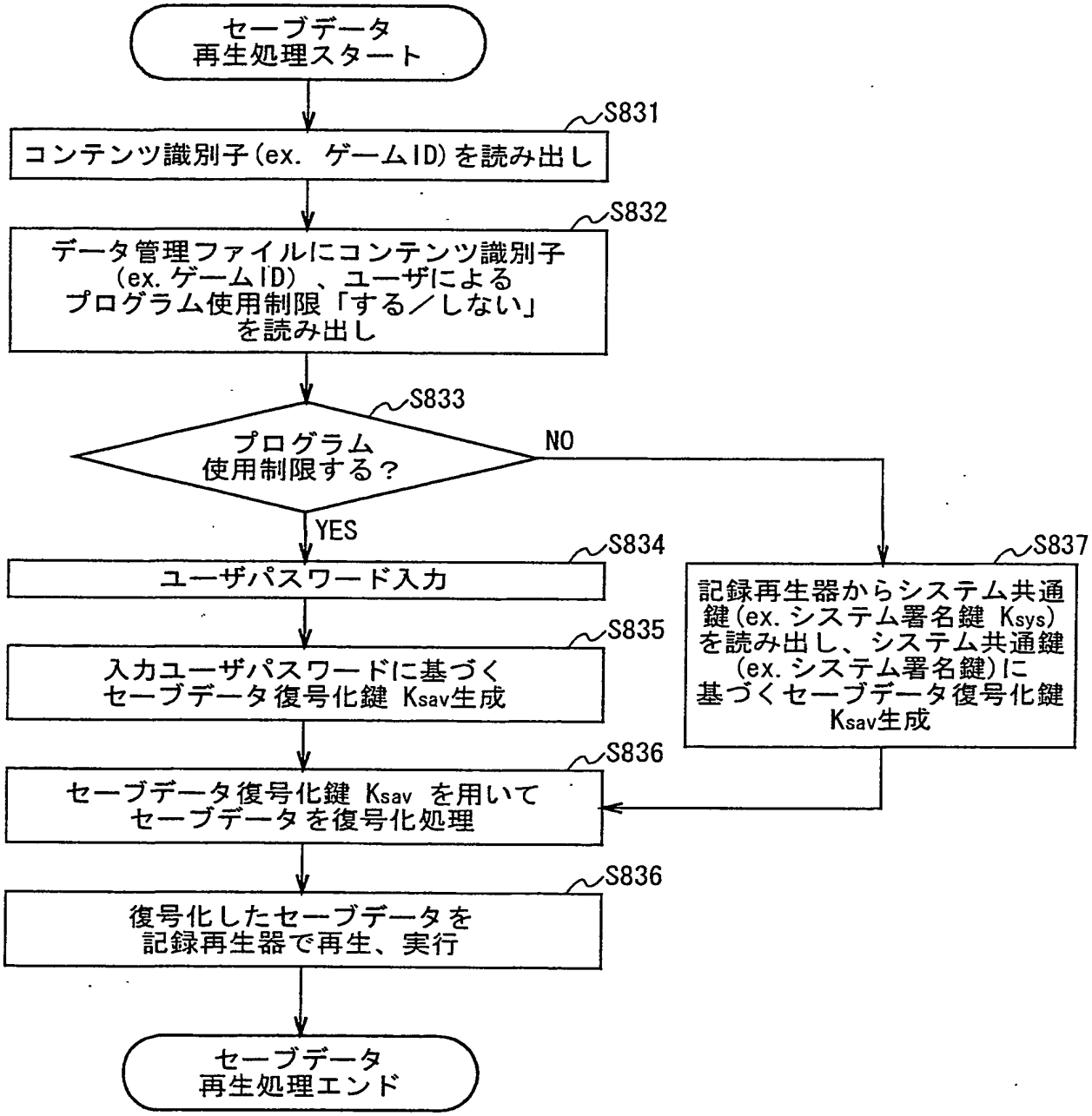


図８５

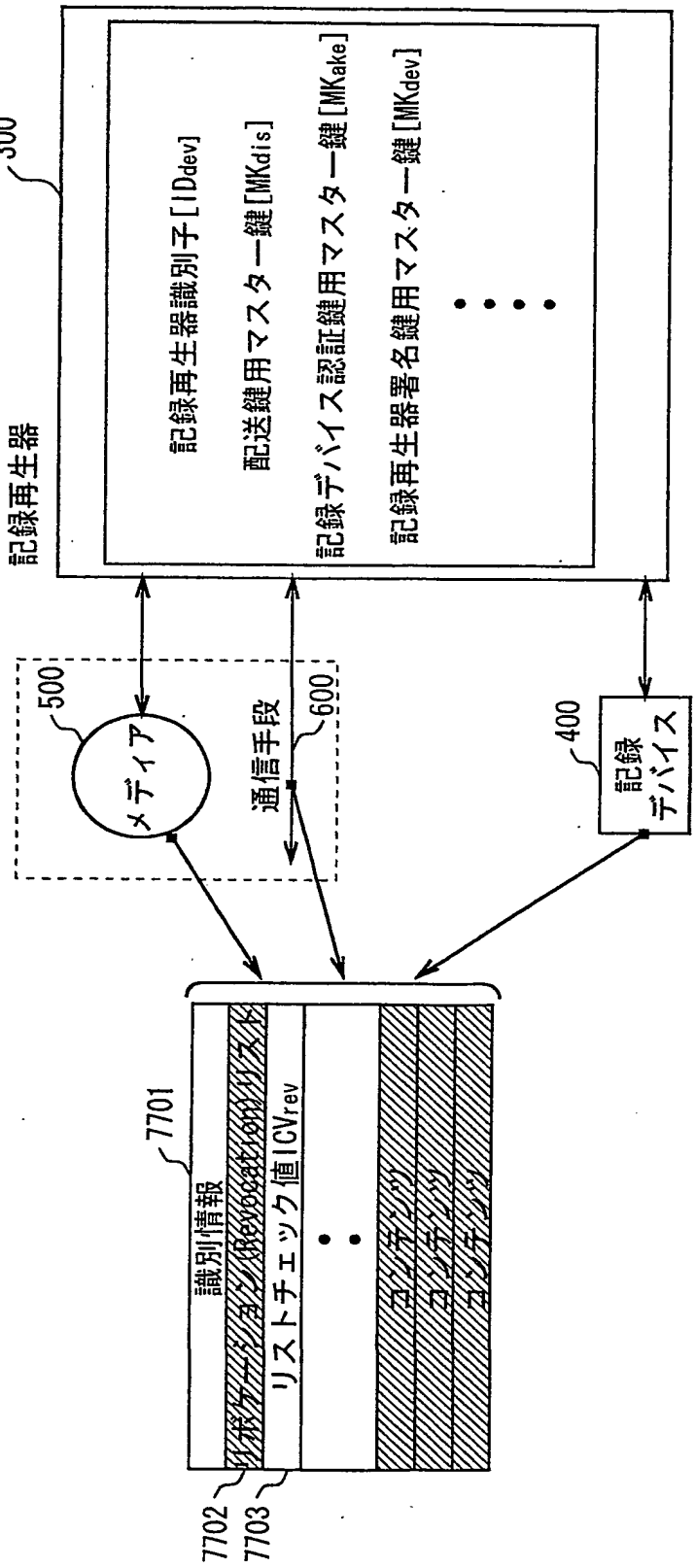

300
記録再生器
記録再生器識別子[IDdev]
配送鍵用マスター鍵[MKdis]
記録デバイス認証鍵用マスター鍵[MKake]
記録再生器署名鍵用マスター鍵[MKdev]
500
メディア
600
通信手段
400
記録デバイス
7701
識別情報
リボケーションリストのバージョン
リストチェック値ICVrev
コンテンツ
コンテンツ
コンテンツ
7702
7703

図86

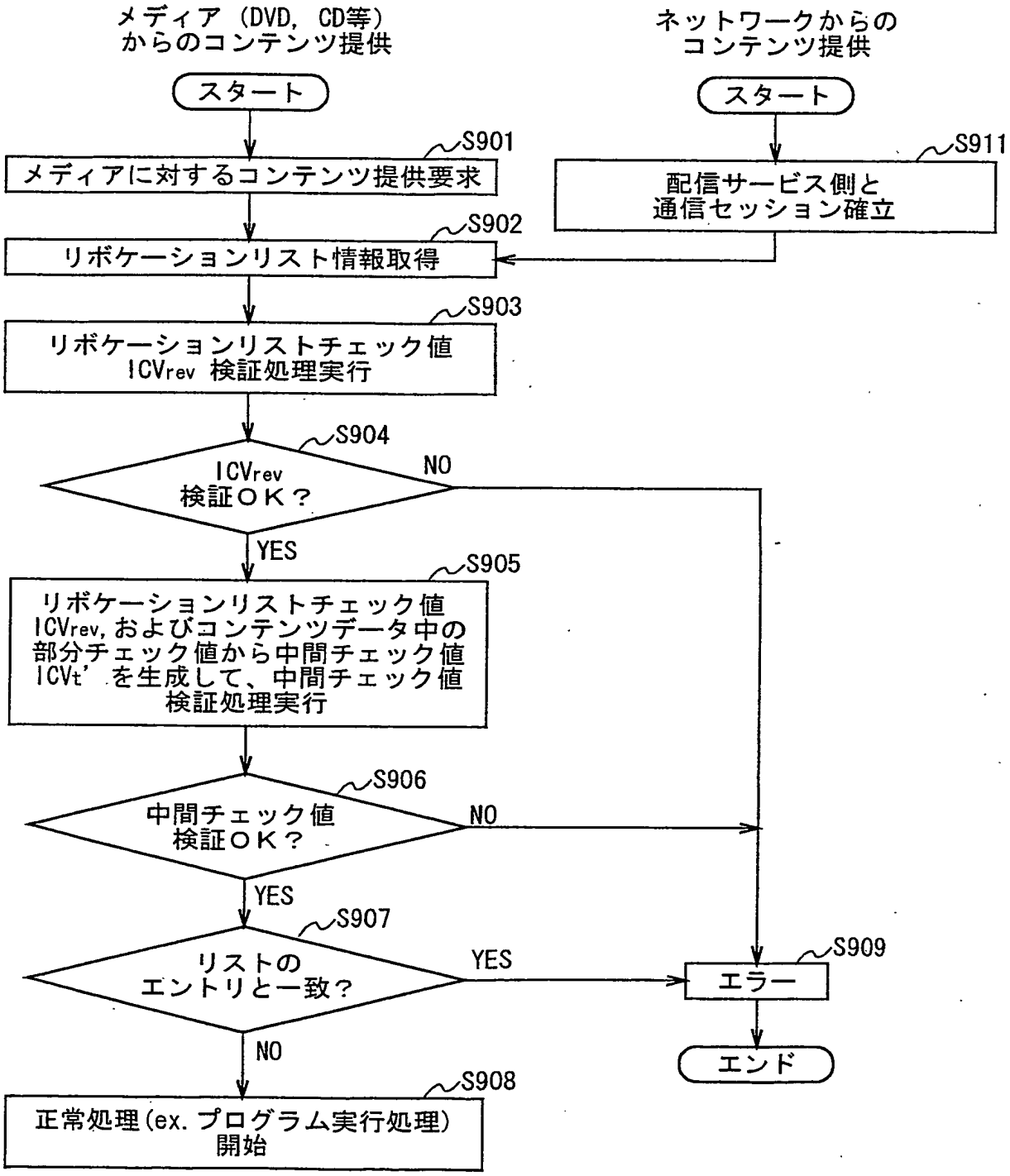

メディア（DVD, CD等）からのコンテンツ提供
ネットワークからのコンテンツ提供
スタート
スタート
S901
メディアに対するコンテンツ提供要求
S911
配信サービス側と通信セッション確立
S902
リボケーションリスト情報取得
S903
リボケーションリストチェック値 ICVrev 検証処理実行
S904
ICVrev 検証ＯＫ？
NO
YES
S905
リボケーションリストチェック値 ICVrev, およびコンテンツデータ中の部分チェック値から中間チェック値 ICVt' を生成して、中間チェック値検証処理実行
S906
中間チェック値 検証ＯＫ？
NO
YES
S907
リストのエントリと一致？
YES
S909
エラー
エンド
NO
S908
正常処理(ex. プログラム実行処理)開始

図８７

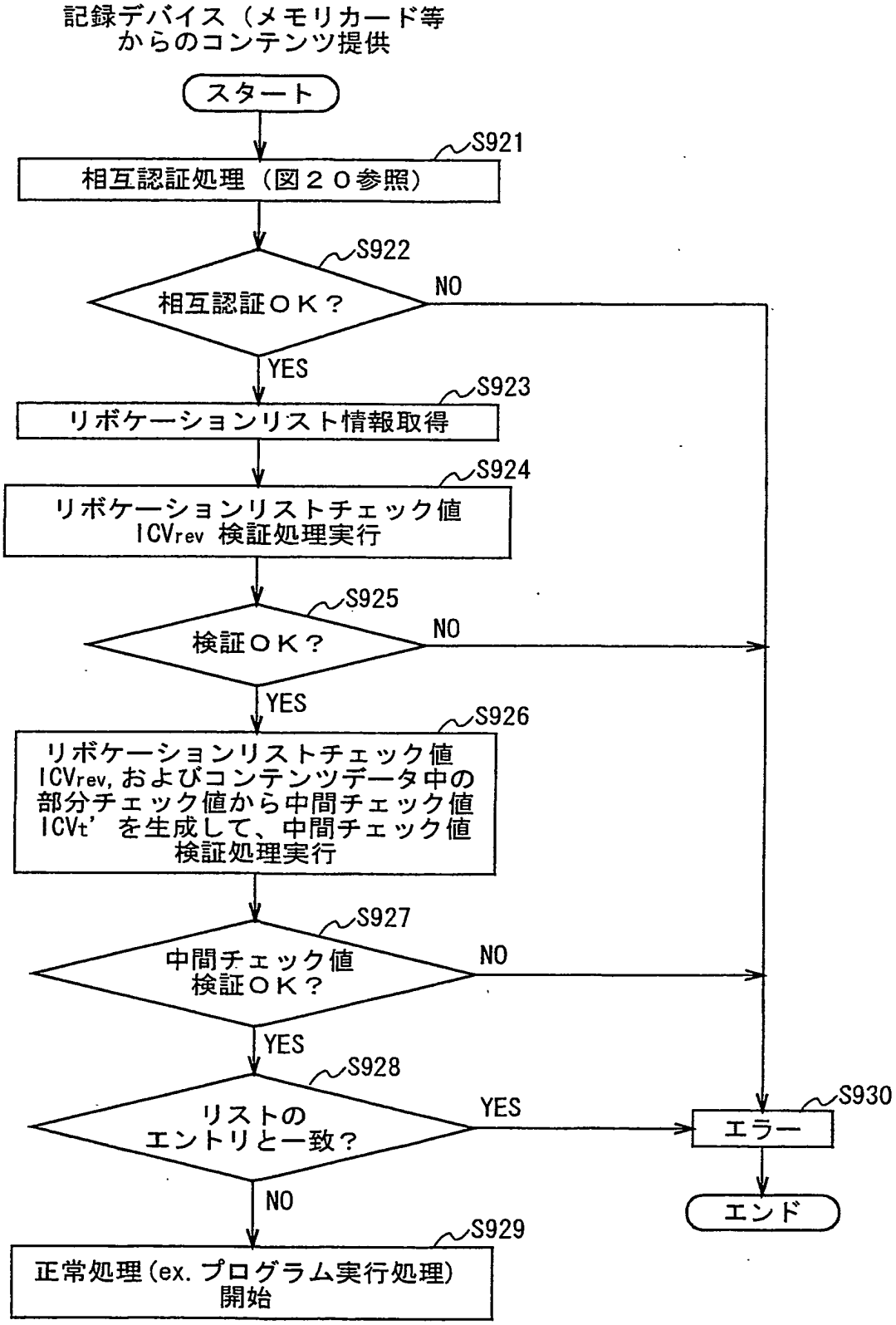
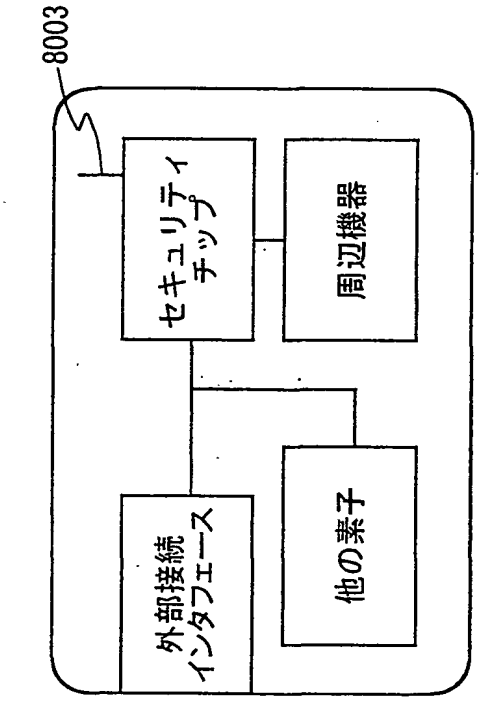
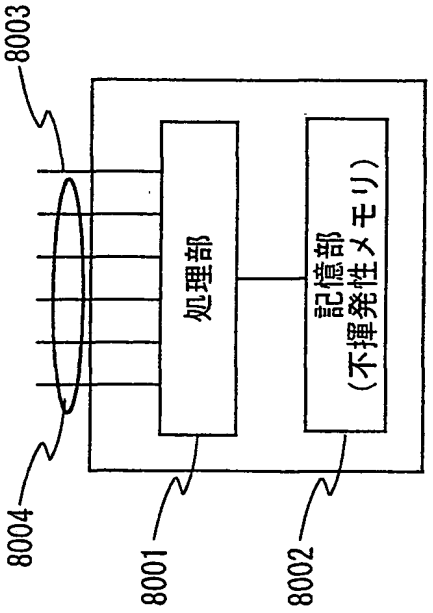

記録デバイス（メモリカード等からのコンテンツ提供
スタート
S921
相互認証処理（図２０参照）
S922
相互認証ＯＫ？
NO
YES
S923
リボケーションリスト情報取得
S924
リボケーションリストチェック値 ICVrev 検証処理実行
S925
検証ＯＫ？
NO
YES
S926
リボケーションリストチェック値 ICVrev, およびコンテンツデータ中の部分チェック値から中間チェック値 ICVt' を生成して、中間チェック値検証処理実行
S927
中間チェック値検証ＯＫ？
NO
YES
S928
リストのエントリと一致？
YES
S930
エラー
エンド
NO
S929
正常処理(ex. プログラム実行処理)開始

図８８



（B）セキュリティチップ搭載製品
（ex. 記録再生器、記録デバイス）



（A）セキュリティチップ
（製造過程）

図89

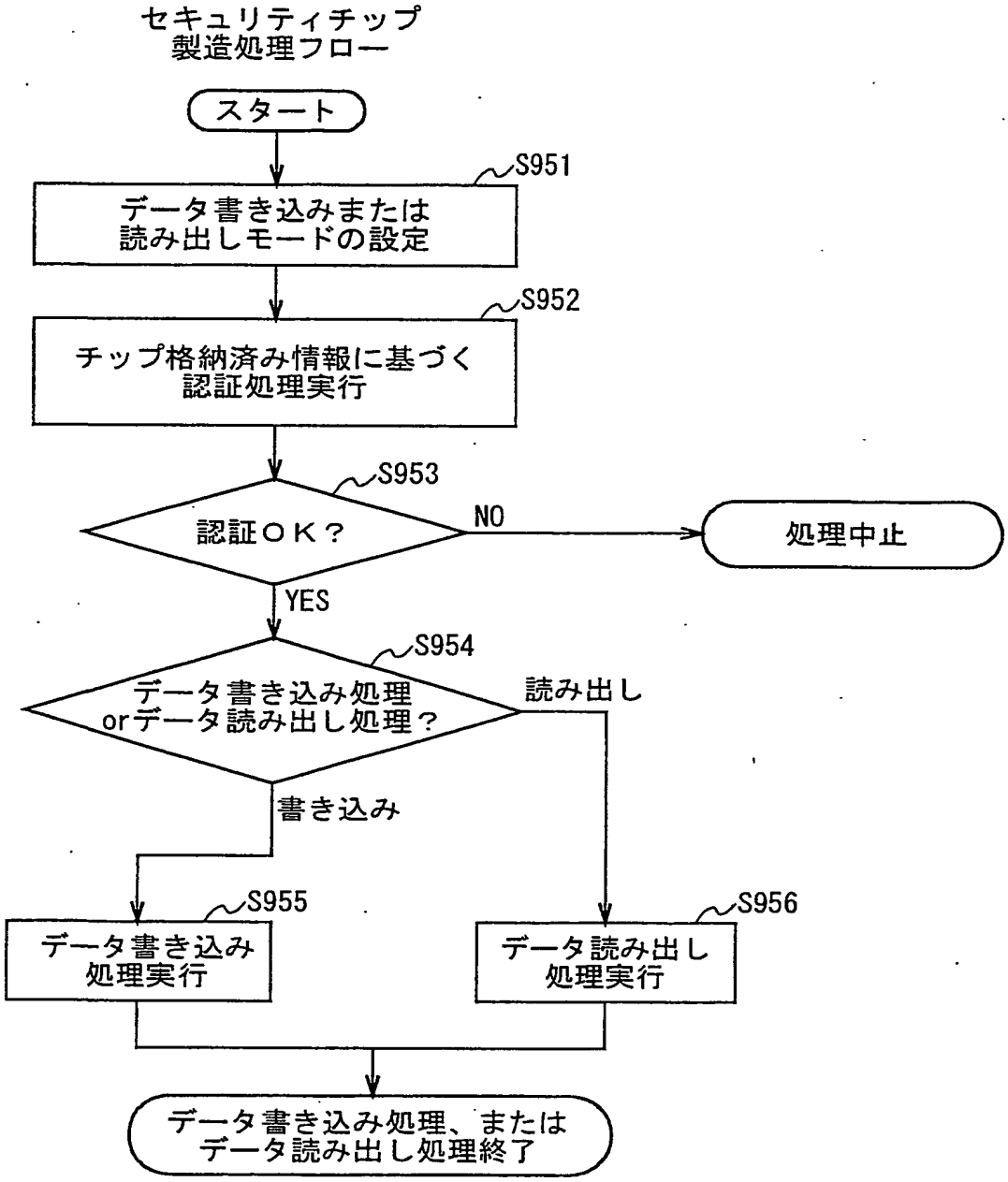
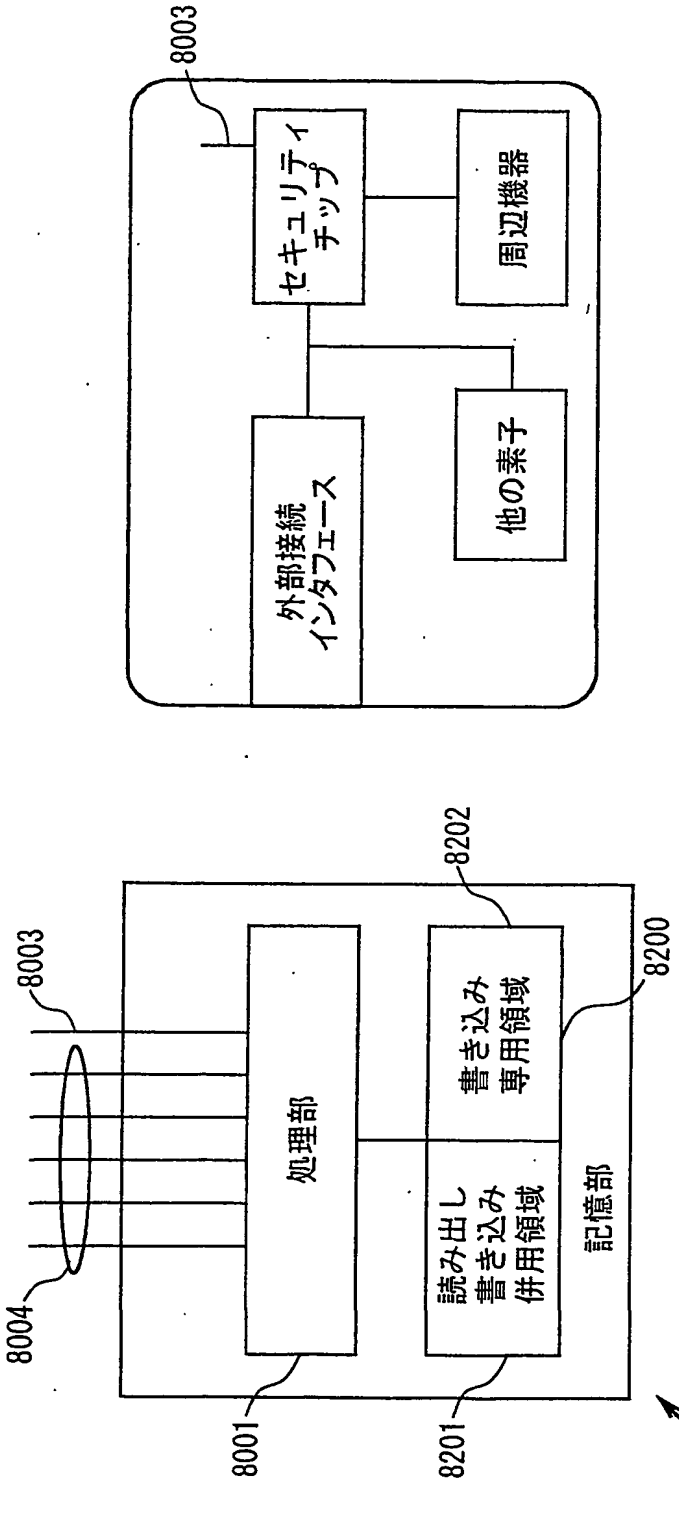

セキュリティチップ
製造処理フロー
スタート
S951
データ書き込みまたは
読み出しモードの設定
S952
チップ格納済み情報に基づく
認証処理実行
S953
認証ＯＫ？
NO
処理中止
YES
S954
データ書き込み処理
orデータ読み出し処理？
読み出し
書き込み
S955
データ書き込み
処理実行
S956
データ読み出し
処理実行
データ書き込み処理、または
データ読み出し処理終了

図９０



（B）セキュリティチップ搭載製品
（ex. 記録再生器、記録デバイス）

（A）セキュリティチップ
（製造過程）

図９１

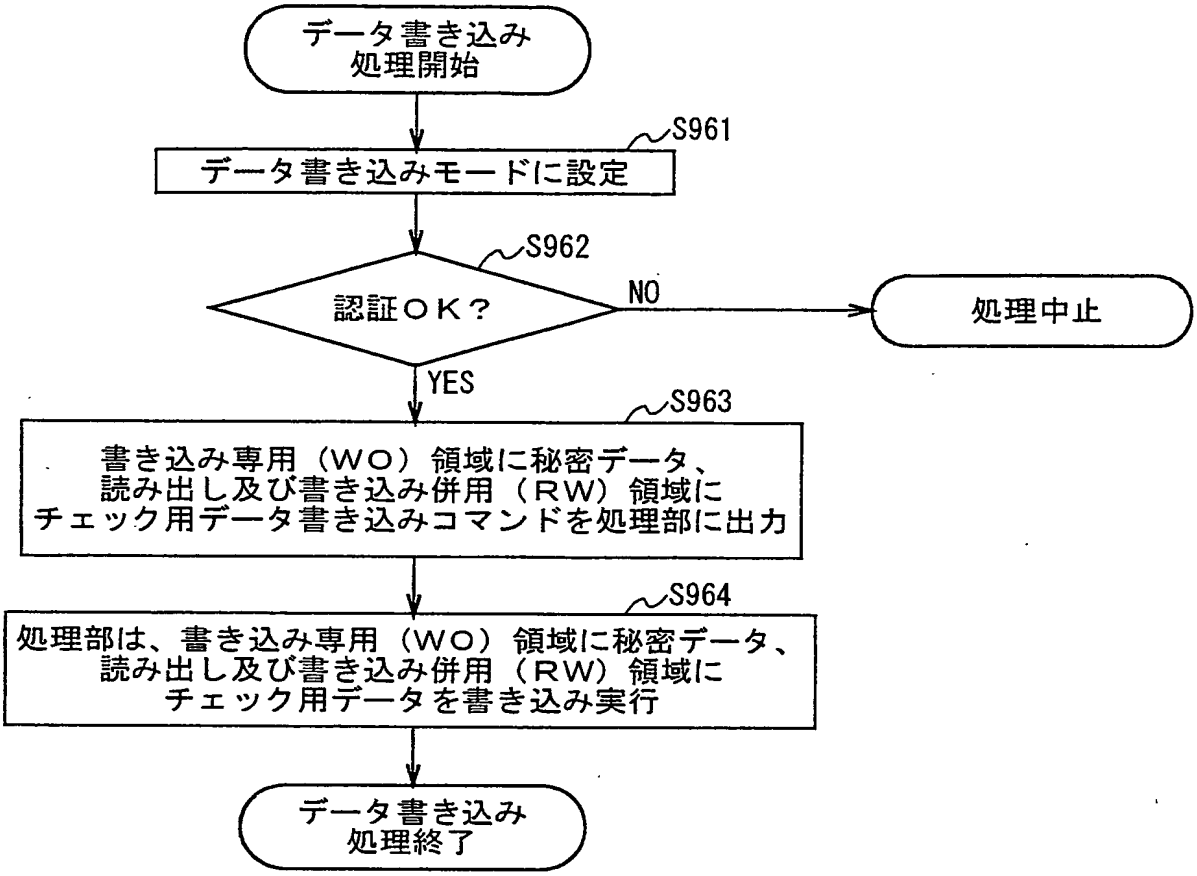

データ書き込み
処理開始
S961
データ書き込みモードに設定
S962
認証ＯＫ？
NO
処理中止
YES
S963
書き込み専用（ＷＯ）領域に秘密データ、
読み出し及び書き込み併用（ＲＷ）領域に
チェック用データ書き込みコマンドを処理部に出力
S964
処理部は、書き込み専用（ＷＯ）領域に秘密データ、
読み出し及び書き込み併用（ＲＷ）領域に
チェック用データを書き込み実行
データ書き込み
処理終了

図９２

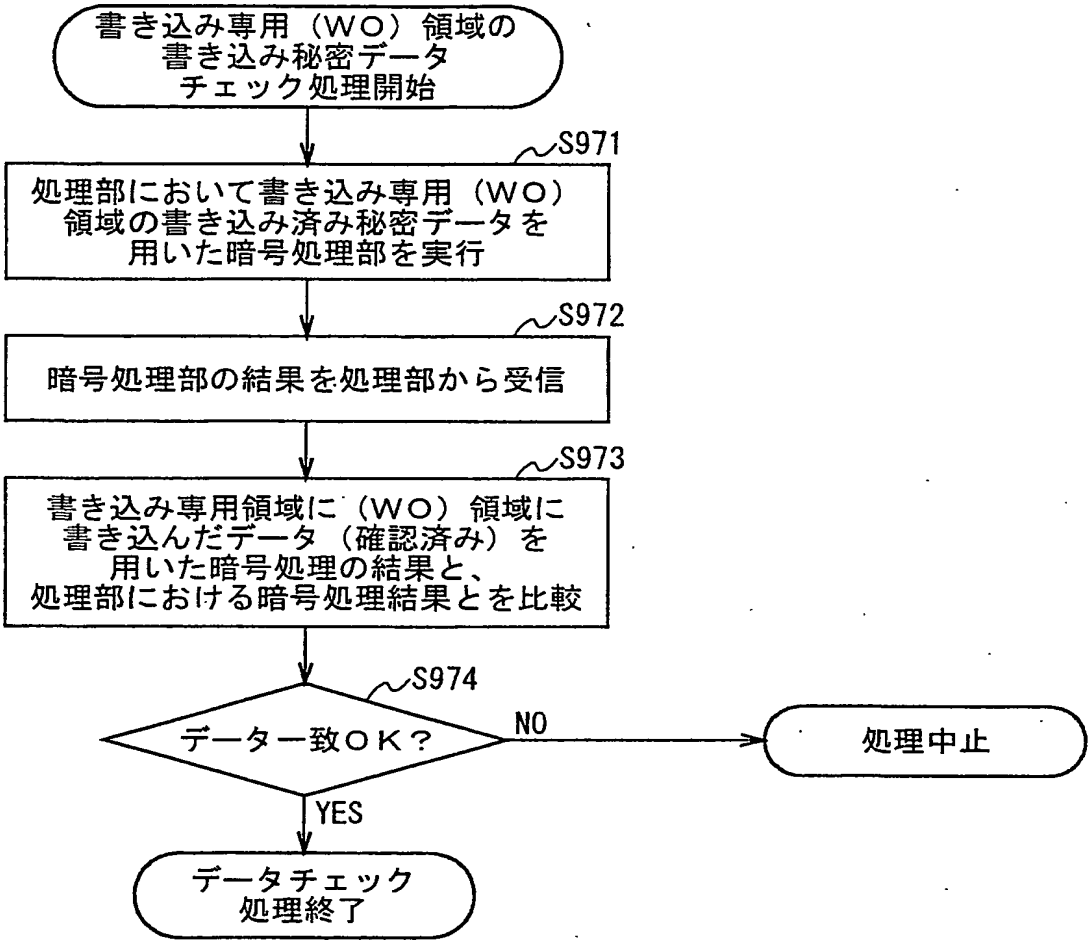

書き込み専用（WO）領域の
書き込み秘密データ
チェック処理開始
S971
処理部において書き込み専用（WO）
領域の書き込み済み秘密データを
用いた暗号処理部を実行
S972
暗号処理部の結果を処理部から受信
S973
書き込み専用領域に（WO）領域に
書き込んだデータ（確認済み）を
用いた暗号処理の結果と、
処理部における暗号処理結果とを比較
S974
データ一致ＯＫ？
NO
処理中止
YES
データチェック
処理終了

図９３

符号の説明

１０６...メインＣＰＵ、１０７...ＲＡＭ、１０８...ＲＯＭ、１０９...ＡＶ処理部、１１０...入力処理部、１１１...ＰＩＯ、１１２...ＳＩＯ、３００...記録再生器、３０１...制御部、３０２...暗号処理部、３０３...記録デバイスコントローラ、３０４...読み取り部、３０５...通信部、３０６...制御部、３０７...内部メモリ、３０８...暗号／復号化部、４００...記録デバイス、４０１...暗号処理部、４０２...外部メモリ、４０３...制御部、４０４...通信部、４０５内部メモリ、４０６...暗号／復号化部、４０７...外部メモリ制御部、５００...メディア、６００...通信手段、２１０１，２１０２，２１０３...記録再生器、２１０４，２１０５，２１０６...記録デバイス、２９０１...コマンド番号管理部、２９０２...コマンドレジスタ、２９０３，２９０４...認証フラグ、３００１...スピーカ、３００２...モニタ、３０９０...メモリ、３０９１...コンテンツ解析部、３０９２...データ記憶部、３０９３...プログラム記憶部、３０９４...圧縮伸長処理部、７７０１...コンテンツデータ、７７０２...リボケーションリスト、７７０３...リストチェック値、８０００...セキュリティチップ、８００１...処理部、８００２...記憶部、８００３...モード信号線、８００４...コマンド信号線、８２０１...読み出し書き込み併用領域、８２０２...書き込み専用領域